GALOIS MODULES, IDEAL CLASS GROUPS AND CUBIC STRUCTURES

GEORGIOS PAPPAS*

Abstract. We establish a connection between the theory of cyclotomic ideal class groups and the theory of "geometric" Galois modules and obtain results on the Galois module structure of coherent cohomology groups of Galois covers of varieties over **Z**. In particular, we show that an invariant that measures the obstruction to the existence of a virtual normal integral basis for the coherent cohomology of such covers is annihilated by a product of certain Bernoulli numbers with orders of even K-groups of **Z**. We also show that the existence of such a normal integral basis is closely connected to the truth of the Kummer-Vandiver conjecture for the prime divisors of the degree of the cover. Our main tool is a theory of "hypercubic structures" for line bundles over group schemes.

Contents

§1. Introduction
§2. Torsors
§3. Hypercubic structures
§4. Multiextensions
§5. Differences and Taylor expansions
§6. Multiextensions and abelian sheaves
§7. Multiextensions of finite multiplicative group schemes
§8. Reflection homomorphisms
§9. The hypercubic structure on the determinant of cohomology
§10. The multiextension associated to a $\mathbf{Z}/p\mathbf{Z}$-torsor
§11. Galois module structure
Appendix

Date: February 1, 2008.
*Partially supported by NSF grant DMS02-01140 and by a Sloan Research Fellowship.

1. Introduction

For a given finite group G and an arithmetic variety Y, we associate to each G-torsor X over Y an equivariant Euler characteristic $\chi^P(\mathcal{O}_X)$ in $\mathrm{K}_0(\mathbf{Z}[G])$ (the Grothendieck group of finitely generated projective $\mathbf{Z}[G]$-modules; see both below and also Section 11). In this paper we develop powerful new methods for determining Euler characteristics of such torsors by extending work of Grothendieck, Breen and other authors on cubic structures. Our main goal is to establish a connection between the problem of determining $\chi^P(\mathcal{O}_X)$ and the classical theory of cyclotomic ideal class groups. We then exhibit annihilators of such Euler characteristics $\chi^P(\mathcal{O}_X)$ constructed from the divisors of certain Bernoulli numbers and the orders of even Quillen K-groups of $\mathbf{Z}$ and describe a relation with the Kummer-Vandiver conjecture. To illustrate the power of these techniques, we mention that our main theorems show in particular that if G is abelian and if either $\dim(Y) \leq 4$ or the cover $X \to Y$ is of "Albanese type" (see §11.d) then $2 \cdot \chi^P(\mathcal{O}_X)$ is the class of a free module in $\mathrm{K}_0(\mathbf{Z}[G])$; furthermore if in addition we suppose that G has odd order then we show that $\chi^P(O_X)$ is in fact the class of a free module. Note that these results may be seen as providing higher dimensional counterparts of a result of M. Taylor, which shows if Y is the spectrum of a ring of algebraic integers of a number field K, then the ring of integers of a non-ramified abelian extension of K always has a normal integral basis. It is also important to note that the techniques developed here, together with the Grothendieck-Riemann-Roch theorem, can be used to determine such Euler characteristics even when the G-cover $X \to Y$ has some ramification - see [CPT] for further developments in this direction. Although a number of results in this paper are valid for non-abelian groups, our approach provides the strongest results when the group is abelian; this article therefore naturally raises some fundamental questions for the actions of non-abelian groups.

To better understand the context of our work, and explain the relation with ideal class groups, we first review some standard cyclotomic theory. The Stickelberger relations in the ideal class groups of cyclotomic fields are undoubtedly among the cornerstones of classical algebraic number theory. Hilbert gave the first "Galois module theoretic" proof of these relations for cyclotomic fields generated by a root is of unity of prime order by showing that, in this case, they can deduced from the fact that, for n square free, the primitive n-th root of unity ζ_n gives a normal integral basis for the ring of integers $\mathbf{Z}[\zeta_n]$ in the cyclotomic field $\mathbf{Q}(\zeta_n)$ (Zahlbericht, Satz 136). Recall that a normal integral basis for the ring of integers $\mathcal{O}_K$ in the Galois extension $K/\mathbf{Q}$ is an algebraic integer $a \in \mathcal{O}_K$ such that $\{\sigma(a)\}_{\sigma\in \mathrm{Gal}(K/\mathbf{Q})}$ give a $\mathbf{Z}$-basis of $\mathcal{O}_K$; alternatively, we can say that a is a normal integral basis when it is a generator of $\mathcal{O}_K$ as a $\mathbf{Z}[\mathrm{Gal}(K/\mathbf{Q})]$-module. This proof of the Stickelberger relations was later extended by Fröhlich to composite f [F1]. Conversely, the Stickelberger relations play a central role in the study of the problem of existence of a normal integral basis: Indeed, Fröhlich uses the prime factorization of the Gauss sum which underlies the Stickelberger relation, to establish his fundamental relation between Galois Gauss sums and tame local resolvents (see [F2] Theorem 27 and VI §4). In the present paper, we extend this classical

connection between the structure of ideal class groups of cyclotomic fields and the theory of "additive" Galois modules in a new direction by considering Galois covers of higher dimensional algebraic varieties over the integers.

Let Y be a projective algebraic variety over $\mathbf{Z}$ (i.e an integral scheme which is projective and flat over $\mathrm{Spec}\,(\mathbf{Z})$). We will consider finite Galois covers $\pi : X \to Y$ with group G. By definition, these covers are everywhere unramified, i.e π is a G-torsor (see §2). The Galois modules we are considering are the finitely generated G-modules $\mathrm{H}^i(X, \mathcal{O}_X)$; more generally we will also consider $\mathrm{H}^i(X, \mathcal{F})$ where $\mathcal{F}$ is a G-equivariant coherent sheaf on X (see §2.c). These (coherent) cohomology groups can be calculated as the cohomology groups of a complex $\mathbf{R}\Gamma(X, \mathcal{F})$ in the derived category of complexes of modules over the group ring $\mathbf{Z}[G]$. The appropriate generalization of the question of the existence of a normal integral basis is now the question:

Is the complex $\mathbf{R}\Gamma(X, \mathcal{F})$ in the derived category of complexes of $\mathbf{Z}[G]$-modules isomorphic to a bounded complex of finitely generated *free* $\mathbf{Z}[G]$-modules?

This question has first been considered in a geometric context by Chinburg [C] for more general (tamely ramified) covers. He showed that the obstruction to a positive answer is an element $\bar{\chi}^P(\mathcal{F})$ ("the projective equivariant Euler characteristic") in the class group $\mathrm{Cl}(\mathbf{Z}[G]) = \mathrm{K}_0(\mathbf{Z}[G])/\pm\{\text{free classes}\}$ of finitely generated projective $\mathbf{Z}[G]$-modules. In [P] we stated the expectation that, for unramified covers, this obstruction should vanish "most of the time" and we obtained results which point in this direction when Y is an arithmetic surface (i.e of dimension 2). In this paper, we extend the results of [P] to varieties of arbitrary dimension. In particular, we show that class field theory combined with results on ideal class groups of cyclotomic fields and their relation with the Quillen K-groups $\mathrm{K}_m(\mathbf{Z})$ (Herbrand's theorem, work of Soulé, Kurihara and others) implies general vanishing theorems for the classes $\bar{\chi}^P(\mathcal{F})$. In fact, as we will explain below, our results indicate that it is reasonable to expect that a positive answer to the above question for all unramified Galois covers $X \to Y$ of prime order $p > \dim(Y)$ is equivalent to the truth of the Vandiver conjecture for p. Vandiver's conjecture (sometimes also attributed to Kummer) for the prime number p is the statement that p does not divide the class number $h_p^+ = \#\mathrm{Cl}(\mathbf{Q}(\zeta_p + \zeta_p^{-1}))$. This has been verified numerically for all $p < 12\cdot 10^6$ [BCEM]. However, there is widespread doubt about its truth in general (see the discussion in Washington's book [W], p. 158). Up to date, this conjecture remains one of the most intractable problems in classical algebraic number theory. Note that a simpler connection between Vandiver's conjecture and the "relative" Galois module structure of the ring of integers in the $\mathbf{Z}_p$-extension of $\mathbf{Q}(\zeta_p)$ is already known (see [KMi], [Gr]). Our results lie deeper and in a different direction.

In order to state our main theorem, we now introduce various numbers which feature in the annihilators of our equivariant Euler characteristics. For a given finite group G we set $\epsilon(G) = \gcd(2, \#G)$. Next recall that the k-th Bernoulli number B_k is defined by the powers series identity: $t/(e^t - 1) = \sum_{k=0}^{\infty} B_k t^k/k!$. For a prime p, we denote by $\mathrm{ord}_p(a)$ the highest

power of p that divides $a \in \mathbf{Z}_{>0}$. For $n \geq 2$, let us set

$$e(n) = \begin{cases} \text{numerator}\,(B_n/n) & , \text{ if } n \text{ is even}, \\ \prod_{p,\, p|h_p^+} \text{ord}_p(\#\mathrm{K}_{2n-2}(\mathbf{Z})) & , \text{ if } n \text{ is odd}, \end{cases}$$

where $\mathrm{K}_{2n-2}(\mathbf{Z})$ is the Quillen K-group (by work of Borel [Bo], this is a finite group for $n > 1$). We set

$$M_n(G) = \prod_{k=2}^{n} \Big(\prod_{p|e(k)} \text{ord}_p(\#G) \Big) , \quad M'_n(G) = \prod_{s=1}^{[n/2]} \Big(\prod_{p|e(2s)} \text{ord}_p(\#G) \Big).$$

Thus $M'_n(G)$ is determined solely by the order of the group G and the divisibility properties of Bernoulli numbers; furthermore it follows at once from the definitions that of course $M'_n(G)$ divides $M_n(G)$.

Now let $\mathcal{M}_G$ be a maximal $\mathbf{Z}$-order in $\mathbf{Q}[G]$ which contains $\mathbf{Z}[G]$ and denote by $\mathrm{Cl}(\mathcal{M}_G)$ the class group of finitely generated projective $\mathcal{M}_G$-modules. Tensoring with $\mathcal{M}_G$ over $\mathbf{Z}[G]$ induces a group homomorphism $\mathrm{Cl}(\mathbf{Z}[G]) \to \mathrm{Cl}(\mathcal{M}_G)$. Denote its kernel by $\mathrm{D}(\mathbf{Z}[G])$; this subgroup of $\mathrm{Cl}(\mathbf{Z}[G])$ is independent of the choice of maximal order $\mathcal{M}_G$ ([F2] I §2).

Let $\pi : X \to Y$ be a G-torsor with $h : Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d. Suppose that $\mathcal{F}$ is a G-equivariant coherent sheaf on X.

Theorem 1.1. *a) The multiple $M_{d+1}(G) \cdot \bar{\chi}^P(\mathcal{F})$ belongs to the kernel subgroup $\mathrm{D}(\mathbf{Z}[G])$.*

b) Assume that all the Sylow subgroups of the group G are abelian. Then the multiple $\epsilon(G)M_{d+1}(G) \cdot \bar{\chi}^P(\mathcal{F})$ is trivial in $\mathrm{Cl}(\mathbf{Z}[G])$.

Theorem 1.2. *Assume that all the prime divisors of the order $\#G$ satisfy Vandiver's conjecture. Let us set $C_{d+1}(G) = \gcd(M'_{d+1}(G), 2((d+1)!!))$ with $(d+1)!! = (d+1)!\,d! \cdots 2!$. Then $C_{d+1}(G) \cdot \bar{\chi}^P(\mathcal{F})$ belongs to the kernel subgroup $\mathrm{D}(\mathbf{Z}[G])$. In particular, if all the prime divisors of $\#G$ satisfy Vandiver's conjecture and are larger than $d+1$ then $\bar{\chi}^P(\mathcal{F})$ belongs to the kernel subgroup $\mathrm{D}(\mathbf{Z}[G])$.*

Theorem 1.3. *Suppose that G is abelian.*

a) If $\pi : X \to Y$ is of Albanese type (see §11.d) then $\bar{\chi}^P(\mathcal{F})$ is trivial in $\mathrm{Cl}(\mathbf{Z}[G])$.

b) If $\pi : X_{\mathbf{Q}} \to Y_{\mathbf{Q}}$ is of Albanese type then the multiple $2((d+1)!!) \cdot \bar{\chi}^P(\mathcal{F})$ is trivial in $\mathrm{Cl}(\mathbf{Z}[G])$.

If $Y_{\mathbf{Q}}$ is smooth, has a rational point and $X_{\mathbf{Q}}$ is geometrically connected, the condition that $X_{\mathbf{Q}} \to Y_{\mathbf{Q}}$ is of Albanese type means that the cover is obtained by specializing an isogeny of the Albanese variety of $Y_{\mathbf{Q}}$ (see §11.d).

Note that for $d = 0$, Fröhlich's conjecture (shown by M. Taylor in [Ta]) implies that, for all finite Galois groups G, the class $\bar{\chi}^P(\mathcal{F})$ is 2-torsion and belongs to the kernel subgroup $\mathrm{D}(\mathbf{Z}[G])$. When $d = 1$ (the case of arithmetic surfaces), $M_{d+1}(G) = 1$ for all G; in this case, Theorem 1.1 was shown in [P]. In fact, we also have $M_{d+1}(G) = 1$ for $d = 2, 3$ and all G (see Remark 7.9). In general, if $\#G$ is relatively prime to $N_{d+1} := \prod_{k=2}^{d+1} e(k)$ then

$M_{d+1}(G) = 1$. Note that by a result of Soulé on the size of $\mathrm{K}_{2m}(\mathbf{Z})$ [So] and standard estimates on Bernoulli numbers, there is an effective (although doubly exponential) bound on N_{d+1}.

Corollary 1.4. *Assume that either all the Sylow subgroups of G are abelian and we have $\epsilon(G)M_{d+1}(G) = 1$ or that G is abelian and $\pi : X \to Y$ is of Albanese type. Then the complex $\mathbf{R}\Gamma(X, \mathcal{F})$ is isomorphic in the derived category to a bounded complex of finitely generated free $\mathbf{Z}[G]$-modules.*

Let $\epsilon(G, Y) := \gcd(2, \#G, g(Y_{\mathbf{Q}}))$ where $g(Y_{\mathbf{Q}})$ is the arithmetic genus of the generic fiber of $Y \to \mathrm{Spec}\,(\mathbf{Z})$. When we restrict our attention to $\mathcal{F} = \mathcal{O}_X$ the conclusions of Theorem 1.1 (b) and of Corollary 1.4 can be slightly improved: in these statements, we can replace $\epsilon(G)$ by $\epsilon(G, Y)$.

In a slightly different direction, we can use the above work to obtain the following very down to earth result on Galois modules:

Corollary 1.5. (Projective integral normal basis) *Assume that either all the Sylow subgroups of G are abelian and we have $\epsilon(G)M_{d+1}(G) = 1$ or that G is abelian and $\pi : X \to Y$ is of Albanese type. Also suppose in addition that X is normal. Then there is a graded commutative ring $\oplus_{n\geq 0}A_n$ with (degree 0) G-action such that for each $n > 0$, A_n is a free $\mathbf{Z}[G]$-module and $X \simeq \mathbf{Proj}(\oplus_{n\geq 0}A_n)$ as schemes with G-action.*

To better explain the relation with Vandiver's conjecture we now assume that $G = \mathbf{Z}/p\mathbf{Z}$, p an odd prime. Then the kernel subgroup $\mathrm{D}(\mathbf{Z}[G])$ is trivial and the class group $\mathrm{Cl}(\mathbf{Z}[G])$ coincides with the ideal class group $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$. For simplicity, we will restrict our discussion to $\mathcal{F} = \mathcal{O}_X$. From Theorem 1.2 above we obtain:

Corollary 1.6. *Assume in addition that $G = \mathbf{Z}/p\mathbf{Z}$, $p > d + 1$, and that p satisfies Vandiver's conjecture. Then $\bar{\chi}^P(\mathcal{O}_X) = 0$.*

Denote by ${}_pC$ (resp. C/p) the kernel (resp. the cokernel) of multiplication by p on $C = \mathrm{Cl}(\mathbf{Q}(\zeta_p))$. We use the superscript (k) to denote the eigenspace of ${}_pC$ or C/p on which $\sigma_a \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, $\sigma_a(\zeta_p) = \zeta_p^a$, acts via multiplication by a^k. Recall the classical "reflection" homomorphisms ([W] §10.2)

$$R^{(i)} : \mathrm{Hom}((C/p)^{(1-i)}, \mathbf{Z}/p\mathbf{Z}) \to {}_pC^{(i)}.$$

We continue to assume that $p > \dim(Y)$. Our results actually produce elements $t_i(X/Y) \in \mathrm{Hom}((C/p)^{(1-i)}, \mathbf{Z}/p\mathbf{Z})$, $1 \leq i \leq d + 1$, such that

$$\bar{\chi}^P(\mathcal{O}_X) = \sum_{i=1}^{d+1} R^{(i)}(t_i(X/Y))$$

in $\mathrm{Cl}(\mathbf{Q}(\zeta_p)) = \mathrm{Cl}(\mathbf{Z}[G])$. By class field theory, each element $t_i(X/Y)$ corresponds to an unramified $\mathbf{Z}/p$-extension of $\mathbf{Q}(\zeta_p)$. We may think of them as characteristic classes of the cover $X \to Y$; at least $t_{d+1}(X/Y)$ can be obtained from the cover of generic fibers

$X_{\mathbf{Q}} \to Y_{\mathbf{Q}}$ in a very explicit manner (see §10 where a relation with a cohomological Abel-Jacobi map considered by Bloch and Colliot-Thélène–Sansuc is also explained). When p satisfies Vandiver's conjecture, we have $R^{(i)} = 0$. Hence, $\bar{\chi}^P(\mathcal{O}_X) = 0$. We conjecture that the elements $\{t_{d+1}(X/Y)\}$, $X \to Y$ ranging over all $\mathbf{Z}/p\mathbf{Z}$-torsors with $Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d, generate the group $\mathrm{Hom}((C/p)^{(-d)}, \mathbf{Z}/p\mathbf{Z})$ (this has the flavor of a refined version of a higher dimensional inverse Galois problem). Since $R^{(i)}$ is injective for i odd ([W]), this conjecture has the following (possibly vacuous) implication:

Conjecture 1.7. *Suppose p does not satisfy Vandiver's conjecture. Then there is a $\mathbf{Z}/p\mathbf{Z}$-torsor $\pi : X \to Y$ with $Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension $d < p-1$ such that $\bar{\chi}^P(\mathcal{O}_X) \neq 0$.*

The problem of determining the classes $\bar{\chi}^P(\mathcal{F})$ is very subtle. Indeed, these lie in the finite group $\mathrm{Cl}(\mathbf{Z}[G])$ and cannot be calculated using the known "Riemann-Roch type" theorems that usually neglect torsion information. Instead, our basic tool is the notion of "n-cubic structure" on line bundles over commutative group schemes. This is a generalization of the notion of cubic structure (for $n = 3$) which was introduced by Breen [Br]. Breen's motivation was to explain the properties of the trivializations of line bundles on abelian varieties which are given by the theorem of the cube. The starting point for us is the fact, shown by F. Ducrot [Du], that the determinant of cohomology along a projective and flat morphism $Y \to S$ of relative dimension d essentially supports a $d+2$-cubic structure (see §9). When G is abelian, we deduce that the square of the determinant $\det_{\mathbf{Z}[G]} \mathbf{R}\Gamma(X, \mathcal{O}_X)^{\otimes 2}$ gives a line bundle over $G^D := \mathrm{Spec}\,(\mathbf{Z}[G])$ which supports a $d+2$-cubic structure. We proceed to analyze line bundles with n-cubic structures over the group scheme G^D. We show that they can be understood using "multiextensions". This is a notion which generalizes that of a biextension and already appears in the work of Grothendieck [SGA6]. One of our main technical results is the "Taylor expansion" of §5 that expresses line bundles with n-cubic structures in terms of multiextensions. The Taylor expansion, when applied to the line bundle $\det_{\mathbf{Z}[G]} \mathbf{R}\Gamma(X, \mathcal{O}_X)^{\otimes 2}$, substitutes for a (functorial) Riemann-Roch theorem "without denominators": it provides a formula for the $2((d+1)!!)$-th power of the determinant of the cohomology. (Notice that in the classical Riemann-Roch theorem multiplying both sides by $(d+1)!!$ clears all the denominators; see Remark 9.9.) When $G = \mathbf{Z}/p\mathbf{Z}$, we see that a k-multiextension over $G^D = \mu_p$ is given by an unramified $\mathbf{Z}/p\mathbf{Z}$-extension L of $\mathbf{Q}(\zeta_p)$ such that $\sigma_a \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ acts by conjugation on $\mathbf{Z}/p\mathbf{Z} = \mathrm{Gal}(L/\mathbf{Q}(\zeta_p))$ via multiplication by a^{1-k}. In fact, the elements $t_i(X/Y)$, $1 \leq i \leq d+1$, mentioned above, correspond to i-multiextensions associated naturally to the $d+2$-cubic structure on $\det_{\mathbf{Z}[G]} \mathbf{R}\Gamma(X, \mathcal{O}_X)^{\otimes 2}$. In general, class field theory implies that the group of multiextensions over G^D can always be described using eigenspaces of cyclotomic ideal class groups. We are able to bound the support of the group of multiextensions using results on the corresponding eigenspaces of these class groups. This technique applies directly when G is abelian and to $\mathcal{F} = \mathcal{O}_X$; the case of more general finite groups and general $\mathcal{F}$ follows from these results using Noetherian induction and the localization methods of [P].

The theory developed in this paper also applies to various other situations. Most of the basic set-up easily extends to torsors for a general finite and flat commutative group scheme over an arbitrary Dedekind ring; this leads to results on "relative" Galois module structure. In fact, the technique of cubic structures provides the most precise general method for determining the Galois module structure of abelian covers even when we allow some (tame) ramification. Then one can not expect $\bar{\chi}^P(\mathcal{F})$ to vanish. However, by combining the theory of the present paper with the Grothendieck-Riemann-Roch theorem we can obtain "fixed point formulas" which calculate the classes $\bar{\chi}^P(\mathcal{F})$ via localization on the ramification locus. This is carried out in joint work with T. Chinburg and M. Taylor [CPT2]. Let us mention here that in the present paper we deal with the Galois modules given by the cohomology of general equivariant sheaves. These are significantly more difficult to determine than the virtual Galois module of the Euler characteristic of the de Rham complex which was considered in [CEPT] and [CPT1]. In these references, an important part of the calculation was quickly reduced to the case $d = 0$ which was then treated using the work of Fröhlich and Taylor. Here we are discussing a genuinely higher dimensional problem. In addition, we cannot in general expect a relation with the ϵ-constants of Artin-Hasse-Weil L-functions as in loc. cit. (Although, for curves, one can anticipate a relation of $\bar{\chi}^P(\mathcal{O}_X)$ with the leading terms of Artin-Hasse-Weil L-functions at $s = 1$.) On the negative side, an extension of Theorem 1.1 (b) to the case that G has a non-abelian Sylow appears to be outside the reach of our techniques; this then raises interesting and fundamental questions concerning torsors of non-abelian groups. In particular our results lead us to formulate the following conjecture for arbitrary finite groups:

Conjecture 1.8. *For any $d \geq 1$, there exists an integer $Q(d)$ with the following property: For any finite group G such that $\gcd(\#G, Q(d)) = 1$ and any G-torsor $X \to Y$ with Y projective and flat of relative dimension d, $\bar{\chi}^P(\mathcal{F})$ is trivial in $\mathrm{Cl}(\mathbf{Z}[G])$ for all G-equivariant coherent sheaves $\mathcal{F}$ on X.*

Let us now describe briefly the contents of the various sections of the paper. In §2 we give some background on commutative Picard categories and torsors. In §3 we define the notion of an n-cubic structure on a line bundle over a commutative group scheme. In §4 and §5 we show how we can analyze line bundles with hypercubic structures using multiextensions; these can be thought of as giving derivatives of the hypercubic structure. The "Taylor expansion" of §5 expresses line bundles with hypercubic structures in terms of multiextensions. In §6 we recall the interpretation of multiextensions as extensions in the derived category of abelian sheaves due to Grothendieck and deduce some corollaries. In §7 and §8 we analyze multiextensions of multiplicative group schemes over $\mathbf{Z}$ and relate them to cyclotomic ideal class groups and to the reflection homomorphisms; we deduce results on line bundles with hypercubic structures over $\mathrm{Spec}\,(\mathbf{Z}[G])$. In §9 we explain the results of [Du] on the hypercubic structure on the determinant of cohomology. In §10 we explain how we can calculate the multiextensions derived from the determinant of the cohomology and, in the case of cyclic groups of prime order, give the explicit description of the invariant

$t_{d+1}(X/Y)$ that was referred to above. The proofs of the results stated in this introduction are completed in §11. Finally, in the Appendix we show how an argument due to Godeaux and Serre combined with an "integral" version of Bertini's theorem (based on a theorem of Rumely on the existence of integral points) allows us to construct "geometric" G-torsors $\pi : X \to Y$ with Y regular and $Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d for any finite group G and any integer $d \geq 1$. This is a result of independent interest.

The author would like to thank T. Chinburg, M. Taylor, R. Kulkarni and L. Washington for useful conversations and comments, and F. Ducrot for making available a preliminary version of the preprint [Du].

2. Torsors

2.a. Recall ([SGA4] XVIII, 1.4) that a (commutative) *Picard category* is a non-empty category $\mathcal{P}$ in which all morphisms are isomorphisms and which is equipped with an "addition" functor

$$+\ : \mathcal{P} \times \mathcal{P} \to \mathcal{P}, \quad (p_1, p_2) \mapsto p_1 + p_2,$$

associativity isomorphisms

$$\sigma_{p_1,p_2,p_3} : (p_1 + p_2) + p_3 \xrightarrow{\sim} p_1 + (p_2 + p_3),$$

functorial in p_1, p_2, p_3, and commutativity isomorphisms

$$\tau_{p_1,p_2} : p_1 + p_1 \xrightarrow{\sim} p_2 + p_1$$

functorial in p_1, p_2 which satisfy the following axioms:

(1) For every object p of $\mathcal{P}$ the functor $\mathcal{P} \to \mathcal{P}$; $q \mapsto p + q$ is an equivalence of categories,
(2) $\tau_{p_2,p_1} \cdot \tau_{p_1,p_2} = \mathrm{Id}_{p_1+p_2}$ for all objects p_1, p_2 of $\mathcal{P}$,
(3) (Pentagon Axiom)

$$(\mathrm{Id}_{p_1} + \sigma_{p_2,p_3,p_4}) \cdot \sigma_{p_1,p_2+p_3,p_4} \cdot (\sigma_{p_1,p_2,p_3} + \mathrm{Id}_{p_4}) = \sigma_{p_1,p_2,p_3+p_4} \cdot \sigma_{p_1+p_2,p_3,p_4},$$

for all objects p_1, p_2, p_3, p_4 of $\mathcal{P}$,

(4) (Hexagon Axiom)

$$\sigma_{p_1,p_2,p_3} \cdot \tau_{p_3,p_1+p_2} \cdot \sigma_{p_3,p_1,p_2} = (\mathrm{Id}_{p_1} + \tau_{p_3,p_2}) \cdot \sigma_{p_1,p_3,p_2} \cdot (\tau_{p_3,p_1} + \mathrm{Id}_{p_2})$$

for all objects p_1, p_2, p_3 of $\mathcal{P}$.

A Picard category is always equipped with an "identity object"; this is a pair $(\underline{O}, \epsilon)$ of an object $\underline{O}$ with an isomorphism $\epsilon : \underline{O} + \underline{O} \xrightarrow{\sim} \underline{O}$ which is unique up to unique isomorphism. For every object p of $\mathcal{P}$ there are isomorphisms $p + \underline{O} \xrightarrow{\sim} p \xleftarrow{\sim} \underline{O} + p$. Fix an identity object $(\underline{O}, \epsilon)$ for $\mathcal{P}$. Then for every object p of $\mathcal{P}$ there is an "inverse", i.e a pair $(-p, i_p)$ of an object $-p$ of $\mathcal{P}$ with a "contraction" isomorphism $i_p : p + (-p) \xrightarrow{\sim} \underline{O}$ which is unique up to unique isomorphism (see [SGA4] XVIII for more details). We associate to $\mathcal{P}$ two commutative groups: The group $\pi_0(\mathcal{P})$ of isomorphism classes of objects of $\mathcal{P}$ and

the group $\pi_1(\mathcal{P}) = \mathrm{Aut}_{\mathcal{P}}(\underline{O})$. For every object q of $\mathcal{P}$ the translation functor provides a canonical isomorphism between $\pi_1(\mathcal{P})$ and $\mathrm{Aut}_{\mathcal{P}}(q)$. The symmetry isomorphism $\tau_{p,p}$ of $p+p$ defines an element $\varepsilon(p)$ of $\pi_1(\mathcal{P})$ such that $\varepsilon(p)^2 = 1$; this gives a group homomorphism $\varepsilon : \pi_0(\mathcal{P}) \to \pi_1(\mathcal{P})$. If in addition to the above axioms we have

(s.c.) $\quad \tau_{p,p} = \mathrm{Id}_{p+p}$, for all objects p of $\mathcal{P}$ (i.e if $\varepsilon = 1$),

then we will say that the Picard category is "strictly commutative".

Note that a commutative group defines a "discrete" s.c. Picard category: The objects are the elements of the group, the only morphisms are the identity morphisms and the addition is given by the group law. A non-trivial example of a s.c. Picard category is provided by the category $\mathrm{PIC}(S)$ of invertible $\mathcal{O}_S$-sheaves over a scheme S with morphisms isomorphisms of $\mathcal{O}_S$-modules and with "addition" given by tensor product ([De]). We will also occasionally use the Picard category $\mathrm{PIC}_*(S)$ of "graded" invertible $\mathcal{O}_S$-sheaves on S: The objects here are pairs $(\mathcal{L}, d)$ of an invertible $\mathcal{O}_S$-sheaf together with a (Zariski) locally constant function $d : S \to \mathbf{Z}$. There exist morphisms from $(\mathcal{L}, d)$ to $(\mathcal{M}, e)$ only if $d = e$ and in this case a morphism is an $\mathcal{O}_S$-module isomorphism $\mathcal{L} \xrightarrow{\sim} \mathcal{M}$. The addition is defined by

$$(\mathcal{L}, d) + (\mathcal{M}, e) = (\mathcal{L} \otimes_{\mathcal{O}_S} \mathcal{M}, d + e).$$

This is endowed with the usual associativity morphisms of the tensor product. The commutativity morphism is given by

$$\tau : (\mathcal{L} \otimes_{\mathcal{O}_S} \mathcal{M}, d + e) \to (\mathcal{M} \otimes_{\mathcal{O}_S} \mathcal{L}, e + d) \ ; \quad l \otimes m \mapsto (-1)^{de} m \otimes l,$$

if l and m are sections of $\mathcal{L}$ and $\mathcal{M}$. Notice that $\mathrm{PIC}_*(S)$ *is not a strictly commutative* Picard category; we have $\epsilon((\mathcal{L}, d)) = (-1)^{d^2} = (-1)^d$.

We will use the following:

Lemma 2.1. *([SGA4] VVIII 1.4.3) Let $(P_i)_{i \in I}$ be a family of objects of the s.c. Picard category $\mathcal{P}$. Denote by $e : I \to \mathbf{Z}^{(I)} = \mathrm{Maps}(I, \mathbf{Z})$ the canonical map $e(i)(j) = \delta_{ij}$. Then there exists a map $\Sigma : \mathbf{Z}^{(I)} \to \mathrm{Ob}(\mathcal{P})$, isomorphisms $a_i : \Sigma(e(i)) \xrightarrow{\sim} P_i$ and $a_{\underline{n},\underline{m}} : \Sigma(\underline{n} + \underline{m}) \xrightarrow{\sim} \Sigma(\underline{n}) + \Sigma(\underline{m})$, $\underline{n}$, $\underline{m} \in \mathbf{Z}^{(I)}$, such that the diagrams*

$$\begin{tikzcd}
\Sigma(\underline{n}+\underline{m}+\underline{k}) \arrow[r, "a_{\underline{n},\underline{m}+\underline{k}}"] \arrow[d, equal] & \Sigma(\underline{n}) + \Sigma(\underline{m}+\underline{k}) \arrow[r, "\mathrm{id}+a_{\underline{m},\underline{k}}"] & \Sigma(\underline{n}) + (\Sigma(\underline{m}) + \Sigma(\underline{k})) \\
\Sigma(\underline{n}+\underline{m}+\underline{k}) \arrow[r, "a_{\underline{n}+\underline{m},\underline{k}}"] & \Sigma(\underline{n}+\underline{m}) + \Sigma(\underline{k}) \arrow[r, "a_{\underline{n},\underline{n}}+\mathrm{id}"] & (\Sigma(\underline{n}) + \Sigma(\underline{m})) + \Sigma(\underline{k}) \arrow[u, "\sigma"']
\end{tikzcd}$$

and,

$$\begin{tikzcd}
\Sigma(\underline{n}+\underline{m}) \arrow[r, "a_{\underline{n},\underline{m}}"] \arrow[d, equal] & \Sigma(\underline{n}) + \Sigma(\underline{m}) \arrow[d, "\tau"'] \\
\Sigma(\underline{m}+\underline{n}) \arrow[r, "a_{\underline{m},\underline{n}}"] & \Sigma(\underline{m}) + \Sigma(\underline{n})
\end{tikzcd}$$

are commutative. The system $(\Sigma, (a_i), (a_{\underline{n},\underline{m}}))$ is unique up to unique isomorphism and is functorial in $(P_i)_{i \in I}$. □

If $\mathcal{P}$ and $\mathcal{Q}$ are two Picard categories an *additive* functor $F : \mathcal{P} \to \mathcal{Q}$ is a functor equipped with isomorphisms

$$f_{p_1,p_2} : F(p_1) + F(p_2) \xrightarrow{\sim} F(p_1 + p_2)$$

for all objects p_1, p_2 of $\mathcal{P}$ which are functorial in p_1, p_2 and which are compatible with the associativity and commutativity isomorphisms of $\mathcal{P}$ and $\mathcal{Q}$ in the sense that we have

$$f_{p_1,p_2+p_3} \cdot (\mathrm{Id}_{F(p_1)} + f_{p_2,p_3}) \cdot \sigma_{F(p_1),F(p_2),F(p_3)} = \\ = F(\sigma_{p_1,p_2,p_3}) \cdot f_{p_1+p_2,p_3} \cdot (f_{p_1,p_2} + \mathrm{Id}_{F(p_3)}),$$

$$f_{p_2,p_1} \cdot \tau_{F(p_1),F(p_2)} = F(\tau_{p_1,p_2}) \cdot f_{p_1,p_2},$$

for all objects p_1, p_2, p_3 of $\mathcal{P}$.

We refer the reader to [SGA4] XVIII 1.4 for the definitions of a (s.c.) Picard stack over a site $\mathfrak{S}$ and of an additive ($\mathfrak{S}$-)functor between two Picard $\mathfrak{S}$-stacks (these are modeled on the definitions above). There is a construction corresponding to Lemma 2.1 in this context. In our applications, the site $\mathfrak{S}$ will be given by a subcategory of the category of S-schemes (Sch/S) equipped with a Grothendieck topology TOP which is either the fpqc or the fppf topology. In this case, we may think of a Picard $\mathfrak{S}$-stack as a fibered category such that the fiber over each $S' \to S$ is a Picard category, with additive pull-back functors and which satisfies a certain descent condition for both the objects and the morphisms. As before, a commutative group scheme over S gives a "discrete" fpqc or fppf s.c. Picard stack. Very often we will work with the site S_{fppf} of S-schemes which are locally of finite presentation with the fppf topology. If $\phi : T \to S$ is an S-scheme we will denote by $\mathcal{PIC}(T)$ (resp. $\mathcal{PIC}_*(T)$) the Picard S_{fppf}-stack given by (resp. graded) invertible $\mathcal{O}_{T\times_S S'}$-sheaves on the schemes $T \times_S S'$, $S' \to S$ a morphism in S_{fppf}.

2.b. Let $H \to S$ be a group scheme *flat and affine over* S. A H-torsor (or "a torsor for H") is a sheaf T for the fpqc topology on (Sch/S) with morphisms

$$m : T \times_S H \to T \ ; \quad m(t,h) = t \cdot h$$

and $p : T \to S$ such that

a) H operates on T (via m) over S.

b) The map $T \times_S H \to T \times_S T$ given by $(t,h) \mapsto (m(t,h),t)$ is an isomorphism.

c) p is a sheaf epimorphism.

By [DG] III §4 Prop. 1.9, under our assumption on H, every H-torsor T is representable by an S-scheme which we will also denote by T; furthermore, the resulting morphism of schemes $p : T \to S$ is affine and faithfully flat and identifies S with the (categorical) quotient T/H. In what follows, we will think of torsors as either fpqc sheaves or schemes without making the distinction.

For more details on the following the reader can refer to [DG] III §4. A morphism between two torsors $T_1 \to S$, $T_2 \to S$, is an S-morphism $f : T_1 \to T_2$ which commutes with the H-action; by descent such a morphism is necessarily an isomorphism. If Y is an S-scheme we will occasionally use the expression "$X \to Y$ is an H-torsor" to mean that $X \to Y$ is

a torsor for the group scheme $H_Y := H \times_S Y \to Y$. By the above, if $\pi : X \to Y$ is an H-torsor, then π is affine and flat and identifies Y with the (categorical) quotient X/H. In fact, this quotient is *universal* in the sense that for every base change $S' \to S$, the natural morphism

$$(X \times_S S')/H \to (X/H) \times_S S' \tag{2.1}$$

is an isomorphism. If $H \to S$ is in addition of finite presentation then so is $\pi : X \to Y$.

Assume now in addition that $H \to S$ is commutative; let $T_1 \to S$, $T_2 \to S$ be two H-torsors. We let the group scheme H act on the fiber product $T_1 \times_S T_2$ by $(t_1, t_2) \cdot h = (t_1 \cdot h, t_2 \cdot h^{-1})$. The quotient $(T_1 \times_S T_2)/H$ then gives an H-torsor over S (the action is via $(t_1, t_2) \cdot h = (t_1 \cdot h, t_2))$ which we will denote by $T_1 \cdot T_2$. We can see that there are canonical isomorphisms of H-torsors

$$T_1 \cdot (T_2 \cdot T_3) \simeq (T_1 \cdot T_2) \cdot T_3, \quad T_1 \cdot T_2 \simeq T_2 \cdot T_1. \tag{2.2}$$

The above satisfy the appropriate axioms so that we obtain on the category of H-torsors the structure of a s.c. Picard category. The identity object is given by the *trivial torsor*. This is $H \to S$ with action given by multiplication; there are canonical isomorphisms

$$H \cdot T \simeq T \cdot H \simeq T. \tag{2.3}$$

The *inverse* $T^{-1} \to S$ of an H-torsor $T \to S$ is the same scheme with new action $m^{-1}(t, h) := m(t, h^{-1})$; there are canonical isomorphisms

$$T^{-1} \cdot T \simeq T \cdot T^{-1} \simeq H. \tag{2.4}$$

Denote by $\mathbf{G}_m$ the multiplicative group scheme over S. There is a natural additive equivalence between the category $\mathrm{PIC}(T)$ of invertible $\mathcal{O}_T$-sheaves over an S-scheme T and the category of $\mathbf{G}_{mT}$-torsors on T given by

$$\mathcal{L} \to \underline{\mathrm{Isom}}_{\mathcal{O}_T}(\mathcal{O}_T, \mathcal{L}).$$

(In what follows, for simplicity, we will denote the $\mathbf{G}_{mT}$-torsor associated to the invertible sheaf $\mathcal{L}$ again by $\mathcal{L}$).

2.c. Assume now that G is a finite group; for a scheme S we will denote by G_S the constant group scheme $\sqcup_{g \in G} S$ given by G. When $S = \mathrm{Spec}\,(\mathbf{Z})$ we will often abuse notation and simply write G instead of G_S. Let T be an S-scheme with a right G-action (this is the same as a right G_S-action). We will say that *G acts freely on T* if for every S-scheme S' the action of G on the set of $T(S')$ of S'-points of the S-scheme T is free (i.e all the stabilizers are trivial).

Assume now that $T \to S$ is quasi-projective. Then the quotient T/G exists as a scheme; when in addition G acts freely on T then $\pi : T \to T/G$ is a G-torsor and the morphism π is finite étale ([D-G] III, §2, n° 6). We will continue with these assumptions in the rest of this section.

A coherent (resp. locally free coherent) sheaf of $\mathcal{O}_T$-G–modules $\mathcal{F}$ on T is a coherent (resp. locally free coherent) sheaf of $\mathcal{O}_T$-modules with an action of G compatible with the action of

G on $(T, \mathcal{O}_T)$ in the appropriate sense. We will often use the term G-equivariant coherent (resp. G-equivariant locally free coherent) sheaf on T instead of coherent (resp. locally free coherent) $\mathcal{O}_T$-G–sheaf. Let $\mathcal{F}$ be a G-equivariant coherent sheaf on T and suppose that $V = \operatorname{Spec}(C)$ is an open affine subscheme of T/G. Since π is finite, $U = \pi^{-1}(V)$ is an affine G-equivariant open subscheme of T. The sections $\mathcal{F}(U)$ form a left G-module and since $\mathcal{F}(U)$ is also a C-module, we obtain on it the structure of a left $C[G]$-module. Hence, $\mathcal{F}$ provides us with a coherent sheaf of $\mathcal{O}_{T/G}[G]$-modules on T/G, which we will denote by $\pi_*(\mathcal{F})$. On the other hand, if $\mathcal{G}$ is a coherent (locally free coherent) sheaf of $\mathcal{O}_{T/G}$-modules on T/G, the pull back $\pi^*(\mathcal{G})$ is a G-equivariant coherent (resp. locally free coherent) sheaf on T. The pull-back functor π^* gives an equivalence between the category of coherent (resp. locally free coherent) sheaves on the quotient T/G and the category of G-equivariant coherent (resp. locally free coherent) sheaves on T. Its inverse functor is obtained by taking invariants under G of the direct image π_*. In particular, there are adjunction functor isomorphisms

$$\mathrm{id} \simeq \pi^* \cdot (\pi_*)^G, \quad \mathrm{id} \simeq (\pi_*)^G \cdot \pi^*. \tag{2.5}$$

2.d. Now suppose that in addition G is commutative. Denote by G_S^D the Cartier dual group scheme of G_S; by definition, this represents the sheaf of characters $\underline{\mathrm{Hom}}(G_S, \mathbf{G}_{mS})$. Let $\chi : G \to \Gamma(S', \mathcal{O}_{S'}^*) = \mathbf{G}_m(S')$ be a character with $S' \to S$ an S-scheme; then χ corresponds to an S'-point of G_S^D. If $\mathcal{F}$ is a G-equivariant coherent (resp. locally free coherent) sheaf on T, consider the coherent sheaf $\mathcal{F}_{S'} := \mathcal{F} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'}$ on $T' := T \times_S S'$ obtained by pulling back $\mathcal{F}$ via $\mathrm{pr}_1 : T' = T \times_S S' \to T$. We can use the character χ to define the structure of an $\mathcal{O}_{T'}$-G-module $\mathcal{F}_{S'}(\chi)$ on $\mathcal{F}_{S'}$ by setting:

$$g \cdot (m \otimes a') = g \cdot m \otimes \chi(g)^{-1} a', \tag{2.6}$$

where m, a' stand for sections of $\mathcal{F}$, resp. $\mathcal{O}_{S'}$. Taking the G-invariants $(\pi'_*(\mathcal{F}_{S'}(\chi)))^G$ of the direct image by $\pi' : T' = T \times_S S' \to (T \times_S S')/G = (T/G) \times_S S'$ gives a coherent sheaf on $(T/G) \times_S S'$ which we will denote by $\mathcal{F}_\chi$. Now apply the above to the structure sheaf $\mathcal{O}_T$. The resulting $\chi \mapsto \mathcal{O}_{T,\chi}$ provides us with a functor from the discrete Picard category $G^D(S')$ to the s.c. Picard category $\mathrm{PIC}(S')$.

Recall that, by using the G-action on $\mathcal{O}_T$, we have given on $\pi_*(\mathcal{O}_T)$ the structure of a coherent sheaf of $\mathcal{O}_S[G]$-modules on S; we may think of $\pi_*(\mathcal{O}_T)$ as a coherent $\mathcal{O}_{G_S^D}$-sheaf on G_S^D. Suppose now that $\chi_0 : G \to \mathbf{G}_m(G_S^D)$ is the "universal" G_S^D-valued character obtained from the natural pairing $G_S^D \times_S G_S \to \mathbf{G}_{mS}$. We have

$$\mathcal{O}_{T,\chi_0} \simeq (\pi_*(\mathcal{O}_T) \otimes_{\mathcal{O}_S} \mathcal{O}_{G_S^D})^G = (\pi_*(\mathcal{O}_T)[G])^G$$

with the G-action defined by $g \cdot (\sum_h a_h h) = \sum_h g(a_h) g^{-1} h$. We can see that this gives an isomorphism

$$\mathcal{O}_{T,\chi_0} \simeq \pi_*(\mathcal{O}_T) \tag{2.7}$$

of (invertible) $\mathcal{O}_{G_S^D}$-sheaves on G_S^D.

Now if χ_1, χ_2 are S'-valued characters of G as above, the multiplication morphism $\mathcal{O}_{T'} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_T \to \mathcal{O}_{T'}$ induces a G-equivariant isomorphism

$$\mathcal{O}_{T'}(\chi_1) \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T'}(\chi_2) \xrightarrow{\sim} \mathcal{O}_{T'}(\chi_1\chi_2). \tag{2.8}$$

It follows from (2.5) that, by passing to G-invariants, this gives an isomorphism of invertible $\mathcal{O}_{S'}$-sheaves

$$c_{\chi_1,\chi_2} : \mathcal{O}_{T,\chi_1} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_2} \xrightarrow{\sim} \mathcal{O}_{T,\chi_1\chi_2}. \tag{2.9}$$

We can see that the diagrams

$$\begin{array}{ccc} \mathcal{O}_{T,\chi_1} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_1} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_1} & \xrightarrow{c_{\chi_1,\chi_2}\cdot \mathrm{id}} & \mathcal{O}_{T,\chi_1\chi_2} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_3} \\ {\scriptstyle \mathrm{id}\cdot c_{\chi_2,\chi_3}}\big\downarrow & & \big\downarrow{\scriptstyle c_{\chi_1\chi_2,\chi_3}} \\ \mathcal{O}_{T,\chi_1} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_2\chi_3} & \xrightarrow{c_{\chi_1,\chi_2\chi_3}} & \mathcal{O}_{T,\chi_1\chi_2\chi_3} \end{array} \tag{2.10}$$

and

$$\begin{array}{ccc} \mathcal{O}_{T,\chi_1} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_2} & \xrightarrow{c_{\chi_1,\chi_2}} & \mathcal{O}_{T,\chi_1\chi_2} \\ {\scriptstyle\wr}\big\downarrow & & \big\| \\ \mathcal{O}_{T,\chi_2} \otimes_{\mathcal{O}_{S'}} \mathcal{O}_{T,\chi_1} & \xrightarrow{c_{\chi_2,\chi_1}} & \mathcal{O}_{T,\chi_2\chi_1} \end{array} \tag{2.11}$$

are commutative. (The left vertical arrow in (2.11) is the commutativity isomorphism; in (2.10), for simplicity, we supress in the notation the associativity isomorphism for the tensor product). Therefore the isomorphisms c_{χ_1,χ_2} are compatible with the associativity and commutativity constraints of the source and target commutative Picard categories. Hence, they equip the functor $\chi \mapsto \mathcal{O}_{T,\chi}$ with additivity data. Notice also that for any base change $q : S'' \to S'$ there are natural isomorphisms

$$q^*\mathcal{O}_{T,\chi} \simeq \mathcal{O}_{T,\chi\cdot q}. \tag{2.12}$$

(on the right hand side, we view χ as a morphism $S' \to G_S^D$). These satisfy the usual cocycle condition and they are compatible with the additivity isomorphisms (2.9). Hence, we can view $\chi \mapsto \mathcal{O}_{T,\chi}$ as providing an additive functor

$$G_S^D \to \mathcal{PIC}(S)$$

from the Picard S_{fppf}-stack given by G_S^D to the Picard S_{fppf}-stack of invertible sheaves.

Remark 2.2. As we shall see in §4.a, the above allows us to construct a commutative extension

$$1 \to \mathbf{G}_{mS} \to E \to G_S^D \to 0 \tag{2.13}$$

such that the fiber of E over the S'-point of G_S^D which is given by the character χ is isomorphic to the $\mathbf{G}_{mS'}$-torsor that corresponds to the invertible $\mathcal{O}_{S'}$-sheaf $\mathcal{O}_{T,\chi}$. We will see in §6 that this construction gives an isomorphism between the group $\mathrm{H}^1(S,G)$ of isomorphism classes of G-torsors over S and the group of isomorphism classes of commutative extensions of G_S^D by $\mathbf{G}_{mS}$.

Remark 2.3. Suppose that $G = \mathbf{Z}/n$ and that S is a Noetherian Spec ($\mathbf{Z}[\zeta_n, 1/n]$)-scheme with ζ_n a primitive n-th root of unity.

a) Let us consider $\psi_0 : G \to \mathcal{O}_S^*$ defined by $\psi_0(a) = \zeta_n^a$. In this case, the association $T \mapsto \mathcal{O}_{T,\psi_0}$ gives an equivalence between the category of $\mathbf{Z}/n$-torsors $T \to S$ and the category of pairs $(\mathcal{L}, t)$ of invertible sheaves $\mathcal{L}$ over S with an isomorphism $t : \mathcal{L}^{\otimes n} \xrightarrow{\sim} \mathcal{O}_S$. (For $\mathcal{L} = \mathcal{O}_{T,\psi_0}$, t is given by $\mathcal{O}_{T,\psi_0}^{\otimes n} \simeq \mathcal{O}_{T,\psi_0^n} = \mathcal{O}_{T,1} \simeq \mathcal{O}_S$, where the first isomorphism is obtained using (2.9)). If S is semilocal, we can choose a trivialization $t' : \mathcal{O}_S \xrightarrow{\sim} \mathcal{L}$ and consider $f = t(t'(1)^{\otimes n}) \in \mathcal{O}_S^*$. Then we can see that the isomorphism class of the pair $(\mathcal{L}, t)$ is determined by the "Kummer element" $f \in \mathcal{O}_S^*/(\mathcal{O}_S^*)^n$; this gives the isomorphism of Kummer theory

$$\mathrm{H}^1(S, \mathbf{Z}/n) \xrightarrow{\sim} \mathcal{O}_S^*/(\mathcal{O}_S^*)^n. \tag{2.14}$$

Note that if we replace in the construction ψ_0 by the inverse character ψ_0^{-1}, we obtain (2.14) composed with the homomorphism $f \mapsto f^{-1}$.

b) Suppose that $\phi : S' \to S$ is a finite locally free morphism. If $\mathcal{L}$ is an invertible sheaf over S', then we can define its norm by

$$\mathrm{Norm}_{S'/S}(\mathcal{L}) = \det(\phi_*(\mathcal{L})) \otimes (\det(\phi_*(\mathcal{O}_{S'}))^{-1}$$

(here det simply means highest exterior power). The norm gives an additive functor from the Picard category of invertible sheaves on S' to the Picard category of invertible sheaves on S. For a finite locally free morphism $\phi : S' \to S$ and a $\mathbf{Z}/n$-torsor $T' \to S'$ we can consider the $\mathbf{Z}/n$-torsor over S which corresponds to the pair $(\mathrm{Norm}_{S'/S}(\mathcal{L}), \mathrm{Norm}_{S'/S}(t))$. By the construction of [SGA4] XVIII this corresponds to the "trace" map

$$\mathrm{Tr}_\phi : \mathrm{H}^1(S', \mathbf{Z}/n) \to \mathrm{H}^1(S, \mathbf{Z}/n) \ . \tag{2.15}$$

If S is semilocal then so is S'. The above then shows that the diagram

$$\begin{array}{ccc} \mathrm{H}^1(S', \mathbf{Z}/n) & \xrightarrow{\sim} & \mathcal{O}_{S'}^*/(\mathcal{O}_{S'}^*)^n \\ {\scriptstyle \mathrm{Tr}_\phi}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{Norm}_{S'/S}} \\ \mathrm{H}^1(S, \mathbf{Z}/n) & \xrightarrow{\sim} & \mathcal{O}_S^*/(\mathcal{O}_S^*)^n \end{array} \tag{2.16}$$

commutes.

3. Hypercubic structures

3.a. Let $H \to S$ be a commutative S-group scheme. For $n \geq 1$, we will denote by $H^n := H \times \cdots \times H$ the n-fold fiber product over S (for simplicity, we will often omit the subscript S in the notation of the product). If I is a subset of the index set $\{1, \ldots, n\}$, we will denote by m_I the morphism $H^n \to H$ given on points by $(h_1, \ldots, h_n) \mapsto \sum_{i \in I} h_i$ (if $I = \emptyset$, $m_I(h_1, \ldots, h_n) = 0$). When $I = \{i\}$, then m_I is the i-th projection $p_{i,H} : H^n \to H$. Recall that we identify the s.c. Picard category of invertible sheaves over an S-scheme T with the s.c. Picard category of $\mathbf{G}_{mT}$-torsors on T (see 2.b). Lemma 2.1 implies that the

"tensor operations" we use in what follows to define invertible sheaves or $\mathbf{G}_m$-torsors give results that are well-defined up to coherent canonical isomorphism.

If $\mathcal{L}$ is an invertible sheaf on H, then we set

$$\Theta_n(\mathcal{L}) = \bigotimes_{I \subset \{1,\ldots,n\}} m_I^*(\mathcal{L})^{(-1)^{n-\#I}} \tag{3.1}$$

(an invertible sheaf on H^n). A permutation $\sigma : \{1,\ldots,n\} \to \{1,\ldots,n\}$ induces a corresponding S-isomorphism $\sigma : H^n \to H^n$. Since $m_I \cdot \sigma = m_{\sigma(I)}$ permuting the factors of 3.1 gives a canonical isomorphism

$$\mathfrak{P}_\sigma : \sigma^*\Theta_n(\mathcal{L}) \xrightarrow{\sim} \Theta_n(\mathcal{L}) \ . \tag{3.2}$$

Now suppose that $n \geq 2$ and consider the morphisms $A, B, C, D : H^{n+1} \to H^n$ given by

$$A(h_0, h_1, h_2, \ldots, h_n) = (h_0 + h_1, h_2, \ldots, h_n), \tag{3.3}$$

$$B(h_0, h_1, h_2, \ldots, h_n) = (h_0, h_1, h_3, \ldots, h_n), \tag{3.4}$$

$$C(h_0, h_1, h_2, \ldots, h_n) = (h_0, h_1 + h_2, h_3, \ldots, h_n), \tag{3.5}$$

$$D(h_0, h_1, h_2, \ldots, h_n) = (h_1, h_2, h_3, \ldots, h_n). \tag{3.6}$$

We can observe that there is a canonical isomorphism

$$\mathfrak{Q} : A^*\Theta_n(\mathcal{L}) \otimes B^*\Theta_n(\mathcal{L}) \xrightarrow{\sim} C^*\Theta_n(\mathcal{L}) \otimes D^*\Theta_n(\mathcal{L}) \tag{3.7}$$

which is obtained by contracting duals and permuting factors (cf. [Br] §2 or [AHS] §2). (The order in which these operations are performed in the s.c. Picard category is of no consequence; the isomorphism remains the same. This can be viewed as a consequence of Lemma 2.1.)

Finally observe that if $(0,\ldots,0) : S \to H^n$ is the zero section, there is a canonical isomorphism

$$\mathfrak{R} : (0,\ldots,0)^*\Theta_n(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_S \ . \tag{3.8}$$

Definition 3.1. *Let $n \geq 2$. An n-cubic structure on the invertible sheaf $\mathcal{L}$ over H is an isomorphism of invertible sheaves on H^n*

$$\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L}) \tag{3.9}$$

(i.e a choice of a global generator $\xi(1)$ of $\Theta_n(\mathcal{L})$) which satisfies the following conditions:

c0) It is "rigid", i.e if $(0,\ldots,0) : S \to H^n$ is the zero section, then

$$\mathfrak{R}((0,\ldots,0)^*(\xi(1))) = 1 \ .$$

c1) It is "symmetric", i.e for all $\sigma \in S_n$,

$$\mathfrak{P}_\sigma(\sigma^*(\xi(1))) = \xi(1) \ .$$

c2) It satisfies the "cocycle condition"

$$\mathfrak{Q}(A^*(\xi(1)) \otimes B^*(\xi(1))) = C^*(\xi(1)) \otimes D^*(\xi(1)) \ .$$

Remark 3.2. a) This definition also appears in [AHS] 2.39. For $n = 3$ it is a slight variant of Breen's definition of a cubic structure ([Br] §2; see also Moret-Bailly [MB]). To explain this set

$$\Theta(\mathcal{L}) := \bigotimes_{\emptyset \neq I \subset \{1,2,3\}} m_I^*(\mathcal{L})^{(-1)^{3-\#I}} = \Theta_3(\mathcal{L}) \otimes m_\emptyset^* \mathcal{L}.$$

(Recall that $m_\emptyset : H^3 \to H$ is the zero homomorphism). There are isomorphisms analogous to (3.2) and (3.7) for $\Theta(\mathcal{L})$. According to Breen, a cubic structure on $\mathcal{L}$ is a trivialization $t : \mathcal{O}_{H^3} \xrightarrow{\sim} \Theta(\mathcal{L})$ which respects these isomorphisms (i.e satisfies conditions analogous to (c1) and (c2)). On the other hand, (3.8) induces a canonical isomorphism

$$0^*\mathcal{L} \xrightarrow{\sim} (0,0,0)^*\Theta(\mathcal{L}).$$

Hence, t also induces a "rigidification" of $\mathcal{L}$, i.e an isomorphism $\mathcal{O}_S \xrightarrow{\sim} 0^*\mathcal{L}$ which we will denote by $r(t)$. For any invertible sheaf $\mathcal{L}$ on H now set $\mathcal{L}^{\mathrm{rig}} := \mathcal{L} \otimes p^* 0^* \mathcal{L}^{-1}$, $p : H \to S$ the structure morphism. The invertible sheaf $\mathcal{L}^{\mathrm{rig}}$ is equipped with a canonical rigidification r_{can} and so there is a canonical isomorphism

$$\phi_{\mathrm{can}} : \Theta_3(\mathcal{L}) \xrightarrow{\sim} \Theta(\mathcal{L}^{\mathrm{rig}}).$$

One can now verify that $\xi \mapsto t(\xi) := \phi_{\mathrm{can}} \cdot \xi$ gives a bijective correspondence between the set of 3-cubic structures ξ on $\mathcal{L}$ in the sense above and the set of Breen's cubic structures t on $\mathcal{L}^{\mathrm{rig}}$ which satisfy $r(t) = r_{\mathrm{can}}$ (cf. [Br] §2.8 and [AHS] Remark 2.44).

b) In what follows, we will often denote various invertible sheaves by giving their fibers over a "general" point of the base. For example, we can denote $\Theta_3(\mathcal{L})$ as

$$\mathcal{L}_{x+y+z} \otimes \mathcal{L}_{x+y}^{-1} \otimes \mathcal{L}_{y+z}^{-1} \otimes \mathcal{L}_{z+x}^{-1} \otimes \mathcal{L}_x \otimes \mathcal{L}_y \otimes \mathcal{L}_z \otimes \mathcal{L}_0^{-1}.$$

(This gives the fiber of $\Theta_3(\mathcal{L})$ over the point (x, y, z) of H^3.)

3.b. i) By definition, an isomorphism between the invertible sheaves with n-cubic structures $(\mathcal{L}, \xi)$ and $(\mathcal{L}', \xi')$ is an isomorphism $\phi : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ such that

$$\Theta_n(\phi) \cdot \xi = \xi' \ ,$$

where $\Theta_n(\phi) : \Theta_n(\mathcal{L}) \xrightarrow{\sim} \Theta_n(\mathcal{L}')$ is functorially induced from ϕ. If $(\mathcal{L}, \xi)$, $(\mathcal{L}', \xi')$ are invertible sheaves with n-cubic structures we define their product

$$(\mathcal{L}, \xi) \cdot (\mathcal{L}', \xi') = (\mathcal{L} \otimes \mathcal{L}', \xi * \xi')$$

where $\xi * \xi'$ is the composition

$$\mathcal{O}_{H^n} = \mathcal{O}_{H^n} \otimes_{\mathcal{O}_{H^n}} \mathcal{O}_{H^n} \xrightarrow{\xi \otimes \xi'} \Theta_n(\mathcal{L}) \otimes_{\mathcal{O}_{H^n}} \Theta_n(\mathcal{L}') \xrightarrow{\alpha} \Theta_n(\mathcal{L} \otimes \mathcal{L}')$$

with α the standard natural isomorphism. We can see that the pairs $(\mathcal{L}, \xi)$ give the objects of a s.c. Picard category n-$\mathrm{CUB}(H, \mathbf{G}_m)$ with arrows given by isomorphisms as above and "addition" given by the above product. (This is similar to the corresponding statement for Breen's cubic structures; see [Br] §2).

ii) Suppose that the invertible sheaf $\mathcal{L}$ on H is trivial via $\psi : \mathcal{O}_H \xrightarrow{\sim} \mathcal{L}$. This then induces a trivialization

$$\Theta_n(\psi) : \mathcal{O}_{H^n} = \Theta_n(\mathcal{O}_H) \xrightarrow{\sim} \Theta_n(\mathcal{L}) \ . \tag{3.10}$$

A second trivialization $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ can now be given via the ratio of the generators

$$c = \xi(1)/\Theta_n(\psi)(1) \in \Gamma(H^n, \mathcal{O}^*_{H^n}) \ . \tag{3.11}$$

In this case, we can see that $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ gives an n-cubic structure on $\mathcal{L}$ if and only if the element c satisfies:

c0) $c(0, \dots, 0) = 1$,

c1) $c(h_{\sigma(1)}, \dots, h_{\sigma(n)}) = c(h_1, \dots, h_n)$, for all $\sigma \in S_n$,

c2) $c(h_0 + h_1, h_2, \dots, h_n)c(h_0, h_1, h_3, \dots, h_n) = c(h_0, h_1 + h_2, h_3, \dots, h_n)c(h_1, h_2, \dots, h_n)$.

(Here h_i, $0 \le i \le n$, range over all T-valued points of H, T any S-scheme. Also, for example, $c(h_1, h_2, \dots, h_n) \in \Gamma(T, \mathcal{O}^*_T)$ is obtained from c by pulling back along the morphism $T \to H^n$ given by $(h_1, h_2, \dots, h_n)$).

An inductive argument shows that if $c \in \Gamma(H^n, \mathcal{O}^*_{H^n})$ satisfies (c0), (c1), (c2) above, then it also satisfies

c0′) $c(h_1, h_2, \dots, h_n) = 1$, if at least one of the h_i is 0.

iii) Suppose that $S = \mathrm{Spec}\,(R)$ and $H = G^D_S$, the Cartier dual of a finite abelian *constant* group scheme G. Then, $H = \mathrm{Spec}\,(R[G])$, $H^n = \mathrm{Spec}\,(R[G \times \cdots \times G])$. If $T = \mathrm{Spec}\,(R')$, then T-valued points $h_i : T \to H$ correspond to R'-valued characters $\chi_i : G \to R'^*$. Suppose now that R is local; then $R[G]$ is semi-local and any invertible sheaf $\mathcal{L}$ on $H = \mathrm{Spec}\,(R[G])$ is trivial. Hence, from (ii), we see that n-cubic structures on $\mathcal{L}$ are given by units $c \in R[G^n]^*$ which satisfy

c0) $(1 \otimes \cdots \otimes 1)(c) = 1$,

c1) $(\chi_{\sigma(1)} \otimes \cdots \otimes \chi_{\sigma(n)})(c) = (\chi_1 \otimes \cdots \otimes \chi_n)(c)$,

c2) $(\chi_0\chi_1 \otimes \chi_2 \otimes \cdots \otimes \chi_n)(c)(\chi_0 \otimes \chi_1 \otimes \chi_3 \otimes \cdots \otimes \chi_n)(c) =$
$(\chi_0 \otimes \chi_1\chi_2 \otimes \chi_3 \otimes \cdots \otimes \chi_n)(c)(\chi_1 \otimes \chi_2 \otimes \cdots \otimes \chi_n)(c)$.

(In these relations $\chi_1 \otimes \cdots \otimes \chi_n$ etc. are characters of G^n which are evaluated on the element c of $R[G^n]$).

As above if $c \in R[G^n]^*$ satisfies (c0), (c1), (c2) above (for all characters of G), then it also satisfies

c0′) $(\chi_1 \otimes \cdots \otimes \chi_n)(c) = 1$, if at least one of the characters χ_i is trivial.

Definition 3.3. *An element c of $R[G^n]$ which satisfies (c0), (c1), (c2) above (for all characters of G) is called* n-cubic.

3.c. Suppose that A is an abelian group and $n \geq 1$. Denote by $I[A]$ the augmentation ideal of the group ring $\mathbf{Z}[A]$; by definition, this is the kernel of the ring homomorphism $\mathbf{Z}[A] \to \mathbf{Z}$; $\sum_a n_a[a] \mapsto \sum_a n_a$. Set

$$C_n(A) := \mathrm{Sym}^n_{\mathbf{Z}[A]} I[A] \tag{3.12}$$

(the n-th symmetric power of the $\mathbf{Z}[A]$-module $I[A]$; cf. [AHS] 2.3.1 where the reader is also referred to for more details). The abelian group $C_n(A)$ is the quotient of $\mathrm{Sym}^n_{\mathbf{Z}} I[A]$ by all the relations of the form

$$\begin{aligned} &([b+a_1]-[b]) \otimes ([a_2]-[0]) \otimes \cdots \otimes ([a_n]-[0]) = \\ &\qquad = ([a_1]-[0]) \otimes ([b+a_2]-[b]) \otimes \cdots \otimes ([a_n]-[0]) \end{aligned}$$

with $a_1, \ldots, a_n, b \in A$. After rearranging and reindexing, this relation can be expressed in terms of the generators $[a_1, \ldots, a_n] := ([a_1]-[0]) \otimes \cdots \otimes ([a_n]-[0])$ of $\mathrm{Sym}^n_{\mathbf{Z}} I[A]$ as

$$\begin{aligned} &[a_1, a_2, \ldots, a_n] + [a_0, a_1 + a_2, a_3, \ldots, a_n] = \\ &\qquad = [a_0, a_1, a_3, \ldots, a_n] + [a_0 + a_1, a_2, \ldots, a_n]. \end{aligned}$$

Now suppose that $A = H(\mathrm{Spec}\,(R'))$, the group of characters of the finite abelian group G with values in the R-algebra R'. We can see by the above that an n-cubic element $c \in R[G^n]^*$ gives a group homomorphism

$$\alpha(c) : C_n(A) \to R'^* \ ; \quad [\chi_1, \ldots, \chi_n] \mapsto (\chi_1 \otimes \cdots \otimes \chi_n)(c)\ . \tag{3.13}$$

In fact, every element $c \in R[G^n]^*$ which satisfies (c0$'$) gives a group homomorphism

$$\bigotimes_{\mathbf{Z}}^{n} I[A] \to R'^*; \qquad ([\chi_1]-[1]) \otimes \cdots \otimes ([\chi_n]-[1]) \mapsto (\chi_1 \otimes \cdots \otimes \chi_n)(c)\ .$$

By the above, if this homomorphism factors through $C_n(A)$ (for all R-algebras R') then c is n-cubic.

4. Multiextensions

4.a. Suppose that J and H are two flat commutative group schemes over the scheme S. We will assume that $J \to S$ is affine. (Most of the time we will take $J = \mathbf{G}_m$ and $H = G^D_S$, the Cartier dual of a finite constant abelian group scheme G_S.) According to [SGA7I] Exposé VII §1 giving a commutative group scheme extension E of H by J is equivalent to giving, for every S-scheme $U \to S$ and each U-point $a : U \to H$ over S, a J_U-torsor E_a with the following additional structure: These torsors should come together with isomorphisms

$$c_{a,a'} : E_a \cdot E_{a'} \xrightarrow{\sim} E_{a+a'} \tag{4.1}$$

such that the diagrams

$$
\text{(4.2)} \qquad
\begin{array}{ccc}
E_a \cdot E_{a'} \cdot E_{a''} & \xrightarrow{c_{a,a'}\cdot \mathrm{id}} & E_{a+a'} \cdot E_{a''} \\
{\scriptstyle \mathrm{id}\cdot c_{a',a''}}\big\downarrow & & {\scriptstyle c_{a+a',a''}}\big\downarrow \\
E_a \cdot E_{a'+a''} & \xrightarrow{c_{a,a'+a''}} & E_{a+a'+a''}
\end{array}
$$

and

$$
\text{(4.3)} \qquad
\begin{array}{ccc}
E_a \cdot E_{a'} & \xrightarrow{c_{a,a'}} & E_{a+a'} \\
\wr\big\downarrow & & \big\| \\
E_{a'} \cdot E_a & \xrightarrow{c_{a',a}} & E_{a'+a}
\end{array}
$$

are commutative. Both the torsors and the isomorphisms should be functorial in the S-scheme U. (Of course, E is then E_{id} for $\mathrm{id} : H \to H$ the "universal" H-point of H.) For simplicity, in the first diagram we write $E_a \cdot E_{a'} \cdot E_{a''}$ instead of using the canonical associativity isomorphism $E_a \cdot (E_{a'} \cdot E_{a''}) \simeq (E_a \cdot E_{a'}) \cdot E_{a''}$. In the second, the left vertical isomorphism is the commutativity isomorphism (see (1.1.4.1) and (1.2.1) in loc. cit.) Another way to describe these conditions is to say that the above data define an additive functor from the discrete Picard category of the abelian group $H(U)$ to the Picard category of J_U-torsors. As a result, when $H \to S$ is fppf, we can view extensions of H by J as being given by additive functors from the discrete Picard S_{fppf}-stack of H to the Picard S_{fppf}-stack of J-torsors (this point of view is explained in more detail in [SGA4] XVIII).

4.b. We refer the reader to [SGA7I] Exposé VII for the definition of J-biextensions of commutative group schemes. There is an obvious generalization of both the notions of extension and biextension: the notion of an n-extension of $(H, \ldots, H)$ by J. (Often, for simplicity, we will just say "n-extension of H by J"; for $n = 1$ this gives a usual extension of commutative group schemes as above and for $n = 2$ a J-biextension of (H, H)). By definition (see loc. cit. Def. 2.1 for $n = 2$ and 2.10.2 in general) such an n-extension is a J-torsor E over H^n equipped with "compatible partial composition laws". Giving an n-extension of $(H, \ldots, H)$ by J is equivalent to giving, for each S-scheme $U \to S$ and U-valued point $(a_1, \ldots, a_n)$ of H^n over S, a J-torsor $E_{(a_1,\ldots,a_n)}$ over U with additional structure: These torsors should come together with isomorphisms $(i = 1, \ldots, n)$

$$
\text{(4.4)} \qquad c^i_{a_1,\ldots,a_i;a'_i,\ldots,a_n} : E_{(a_1,\ldots,a_i,\ldots,a_n)} \cdot E_{(a_1,\ldots,a'_i,\ldots,a_n)} \xrightarrow{\sim} E_{(a_1,\ldots,a_i+a'_i,\ldots,a_n)}
$$

which satisfy conditions as in (4.2), (4.3). In addition, we require the following compatibility requirement between the isomorphisms for various i: For all pairs $i \neq j$, the diagram

$$
\text{(4.5)} \qquad
\begin{array}{ccc}
E_{(a_i,a_j)} \cdot E_{(a'_i,a_j)} \cdot E_{(a_i,a'_j)} \cdot E_{(a'_i,a'_j)} & \xrightarrow{c^i\cdot c^i} & E_{(a_i+a'_i,a_j)} \cdot E_{(a_i+a'_i,a'_j)} \\
{\scriptstyle (c^j\cdot c^j)\circ\phi}\big\downarrow & & {\scriptstyle c^j}\big\downarrow \\
E_{(a_i,a_j+a'_j)} \cdot E_{(a'_i,a_j+a'_j)} & \xrightarrow{c^i} & E_{(a_i+a'_i,a_j+a'_j)}
\end{array}
$$

is commutative. (Here, for simplicity, we write $E_{(b_i,b_j)}$ instead of $E_{(b_1,\dots,b_i,\dots,b_j,\dots,b_n)}$ and omit the subscripts from the notation of the composition laws. Also, we denote by ϕ the canonical isomorphism $E_{(a_i,a_j)}\cdot E_{(a'_i,a_j)}\cdot E_{(a_i,a'_j)}\cdot E_{(a'_i,a'_j)}\simeq E_{(a_i,a_j)}\cdot E_{(a_i,a'_j)}\cdot E_{(a'_i,a_j)}\cdot E_{(a'_i,a'_j)}$.) Once again both the torsors and the isomorphisms should be functorial on the S-scheme U.

In fact, these conditions on (4.4) are such that, for each i, these isomorphisms equip E with a structure of an extension of commutative group schemes over $H\times\cdots\times\underset{i}{\hat{H}}\times\cdots\times H$ (this notation means that the i-th factor is omitted from the product)

$$0\to J_{H\times\cdots\times\underset{i}{\hat{H}}\times\cdots\times H}\to E\to H_{H\times\cdots\times\underset{i}{\hat{H}}\times\cdots\times H}\to 0\ . \tag{4.6}$$

There is an obvious notion of isomorphism between n-extensions of H by J (it is given by an isomorphism of the corresponding torsors that respects the composition laws (4.4)). The n-extensions of H by J form the objects of a strictly commutative Picard category n-$\mathrm{EXT}(H,J)$ with morphisms given by isomorphisms of n-extensions and product corresponding to product of the extensions (4.6). The identity object is given by the "trivial" n-extension on the trivial torsor $J\times_S H^n$. These facts are explained in detail in [SGA7I] Exp. VII §1 and §2 when $n=1,\ 2$. The same constructions apply to the general case (see loc. cit. Remark 3.6.7). We will denote by n-$\mathrm{Ext}^1(H,J)$ the commutative group of isomorphism classes of n-extensions of H by J and by n-$\mathrm{Ext}^0(H,J)$ the commutative group of the endomorphisms of the identity object.

Note that sending the class of an n-extension to the class of the underlying J-torsor over H^n defines a group homomorphism

$$t: n\text{-}\mathrm{Ext}^1(H,J)\to \mathrm{H}^1(H^n,J). \tag{4.7}$$

When $J=\mathbf{G}_m$, we can view this as a homomorphism

$$t: n\text{-}\mathrm{Ext}^1(H,\mathbf{G}_m)\to \mathrm{Pic}(H^n). \tag{4.8}$$

4.c. Suppose that E is an n-extension of H by J. If $\sigma\in S_n$ is a permutation, then we also denote by $\sigma: H^n\to H^n$ the corresponding automorphism. We can see that the pull-back J-torsor σ^*E also supports a canonical structure of an n-extension of H by J. Denote by Δ_n the diagonal homomorphism $H\to H^n$.

We will say that the n-extension E of H by J is *symmetric* if it comes together with isomorphisms of n-extensions

$$\Psi_\sigma:\sigma^*E\xrightarrow{\sim}E,\quad \text{for each } \sigma\in S_n,$$

which satisfy the following properties:

i) $\Delta_n^*\Psi_\sigma=i_\sigma$ where $i_\sigma:\Delta_n^*\sigma^*E\xrightarrow{\sim}\Delta_n^*E$ is the natural isomorphism of J-torsors obtained by $\sigma\cdot\Delta_n=\Delta_n$.

ii) For every pair σ, $\tau \in S_n$, the following diagram is commutative

$$\begin{array}{ccc} \sigma^*(\tau^*E) & \xrightarrow{\sigma^*\Psi_\tau} & \sigma^*E \\ \wr\downarrow & & \downarrow\Psi_\sigma \\ (\tau\sigma)^*E & \xrightarrow{\Psi_{\tau\sigma}} & E \end{array}$$

where the left vertical arrow is the natural isomorphism of J-torsors.

Notice that the trivial n-extension is naturally symmetric. When $n = 1$ every extension is symmetric with $\Psi_{\mathrm{id}} = \mathrm{id}$.

By definition, an isomorphism between two symmetric n-extensions $(E, \{\Psi_\sigma\})$ and $(E', \{\Psi'_\sigma\})$ is an isomorphism $f : E \xrightarrow{\sim} E'$ of n-extensions such that for any $\sigma \in S_n$ the following diagram commutes:

$$\begin{array}{ccc} \sigma^*E & \xrightarrow{\sigma^*f} & \sigma^*E' \\ \Psi_\sigma\downarrow & & \downarrow\Psi'_\sigma \\ E & \xrightarrow{f} & E'. \end{array} \tag{4.9}$$

5. Differences and Taylor expansions

In this section we assume that $S = \mathrm{Spec}\,(R)$ and $H = G_S^D$, the Cartier dual of the finite *constant* group scheme given by the abelian group G. The constructions which we will describe below are certainly valid under less restrictive hypotheses. However, we are only going to need them under these assumptions and so we choose to explain them only in this case since then the presentation simplifies considerably. With the exception of the "Taylor expansion" of §5.c most of them are relatively straightforward generalizations of similar constructions described in [Br] for $n = 3$. We consider the "$n-1$-th symmetric difference" $\Theta_{n-1}(\mathcal{L})$ of the invertible sheaf with an n-cubic structure $(\mathcal{L}, \xi)$ on H. We first show that $\Theta_{n-1}(\mathcal{L})$ is naturally equipped with the structure of an $n-1$-extension and then explain how we can recover a power of $(\mathcal{L}, \xi)$ from such symmetric differences using a Taylor-like expansion.

5.a. Let $n \geq 2$. For $1 \leq i \leq n-1$ consider the morphisms $A_i, B_i, C_i : H^n \to H^{n-1}$ given on points by

$$\begin{aligned} A_i(h_1, h_2, \ldots, h_n) &= (h_1, \ldots, \hat{h}_i, \ldots, h_n), \\ B_i(h_1, h_2, \ldots, h_n) &= (h_1, \ldots, \hat{h}_{i+1}, \ldots, h_n), \\ C_i(h_1, h_2, \ldots, h_n) &= (h_1, \ldots, h_i + h_{i+1}, \ldots, h_n), \end{aligned}$$

where $\hat{h}_j$ means "omit h_j" and where in the last expression $h_i + h_{i+1}$ is placed in the i-th position. If $\mathcal{L}$ is an invertible sheaf on H, we can see from the definitions that there is a canonical isomorphism

$$\Theta_n(\mathcal{L}) \xrightarrow{\sim} C_i^*\Theta_{n-1}(\mathcal{L}) \otimes A_i^*\Theta_{n-1}(\mathcal{L})^{-1} \otimes B_i^*\Theta_{n-1}(\mathcal{L})^{-1}\ . \tag{5.1}$$

Let now $(\mathcal{L}, \xi)$ be an invertible sheaf with an n-cubic structure over H. We will show how we can associate to the pair $(\mathcal{L}, \xi)$ an $n-1$-extension $E(\mathcal{L}, \xi)$ of H by $\mathbf{G}_m$. The corresponding $\mathbf{G}_m$-torsor on H^{n-1} is given by $\Theta_{n-1}(\mathcal{L})$. For $n = 3$ a similar construction is described in [Br] §2; the general cases follows along the same lines. We sketch the argument below: By composing (5.1) with ξ we obtain an isomorphism

$$c^i : A_i^* \Theta_{n-1}(\mathcal{L}) \otimes B_i^* \Theta_{n-1}(\mathcal{L}) \xrightarrow{\sim} C_i^* \Theta_{n-1}(\mathcal{L}) \tag{5.2}$$

of invertible sheaves on H^n. We can verify that these isomorphisms provide the partial composition laws (4.4) of an $n-1$-extension: To check that the c^i are commutative, associative (as in (4.3) and (4.2)) and compatible with each other (as in (4.5)) we can reduce to the case that R is local and $\mathcal{L}$ is the trivial invertible sheaf on H (3.b (ii)-(iii)). Then the n-cubic structure ξ on $\mathcal{L}$ is given by an n-cubic element $c \in R[G^n]^*$ and, by the above, the "composition law" c^i is given via multiplication by the element c. Hence, we are reduced to checking certain identities for c. These follow directly from properties (c1) and (c2) of 3.b (ii). More specifically, the commutativity, resp. associativity, property for c^i follows directly from property (c1), resp. (c2), for c. The compatibility (4.5) between the partial composition laws c^i for various i also follows immediately from (c1) and (c2). As a result, the isomorphisms c^i, $1 \leq i \leq n-1$, provide $\Theta_{n-1}(\mathcal{L})$ with the structure of an $n-1$-extension $E(\mathcal{L}, \xi)$. In fact, we can see that the construction $(\mathcal{L}, \xi) \mapsto E(\mathcal{L}, \xi)$ is functorial and gives an additive functor

$$n\text{-CUB}(H, \mathbf{G}_m) \to (n-1)\text{-EXT}(H, \mathbf{G}_m)\ .$$

Actually, we can see that the $n-1$-extension $E(\mathcal{L}, \xi)$ is symmetric (in the sense of the previous paragraph) with the symmetry isomorphisms Ψ_σ given by the isomorphisms $\mathfrak{P}_\sigma$ of (3.2) ($\sigma \in S_{n-1}$). Indeed, it is easy to see that the isomorphisms $\mathfrak{P}_\sigma$ of $\mathbf{G}_m$-torsors satisfy the conditions (i) and (ii) of 4.c and it remains to show that they actually give (iso)morphisms of $n-1$-extensions. An argument as above now shows (by reducing to the case R local and $\mathcal{L}$ trivial) that this follows from the definitions and property (c1).

5.b. In this paragraph, we assume that $n \geq 3$. Let $\mathcal{L}$ be an invertible sheaf over H equipped with an isomorphism

$$\xi' : \mathcal{O}_{H^{n-1}} \xrightarrow{\sim} \Theta_{n-1}(\mathcal{L})$$

For simplicity, we set $A' = A_1$, $B' = B_1$, $C' = C_1$ for the morphisms $H^n \to H^{n-1}$ of 5.a. Recall the canonical isomorphism (5.1)

$$\Theta_n(\mathcal{L}) \xrightarrow{\sim} C'^* \Theta_{n-1}(\mathcal{L}) \otimes A'^* \Theta_{n-1}(\mathcal{L})^{-1} \otimes B'^* \Theta_{n-1}(\mathcal{L})^{-1}.$$

Define an isomorphism

$$\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L}) \tag{5.3}$$

by composing the inverse of (5.1) with the trivialization of

$$C'^* \Theta_{n-1}(\mathcal{L}) \otimes A'^* \Theta_{n-1}(\mathcal{L})^{-1} \otimes B'^* \Theta_{n-1}(\mathcal{L})^{-1}$$

induced by $\xi' : \mathcal{O}_{H^{n-1}} \xrightarrow{\sim} \Theta_{n-1}(\mathcal{L})$.

Lemma 5.1. *If $(\mathcal{L}, \xi')$ is a line bundle with an $n-1$-cubic structure on H, then ξ given by (5.3) gives an n-cubic structure on $\mathcal{L}$. In fact, the construction $(\mathcal{L}, \xi') \mapsto (\mathcal{L}, \xi)$ gives an additive functor*

$$(n-1)\text{-CUB}(H, \mathbf{G}_m) \to n\text{-CUB}(H, \mathbf{G}_m)\ .$$

PROOF. To show the first statement we have to show that the isomorphism (5.3) above satisfies the conditions (c0), (c1), (c2) of Definition 3.1 for an n-cubic structure. For this purpose, we may assume that R is local and that $\mathcal{L}$ is the trivial invertible sheaf on H (see 3.b (ii)). Then the $n-1$-cubic structure ξ' is given by an $n-1$-cubic element $c' \in R[G^{n-1}]^* = \Gamma(H^{n-1}, \mathcal{O}^*_{H^{n-1}})$ and we can see that ξ is given by $c \in R[G^n]^* = \Gamma(H^n, \mathcal{O}^*_{H^n})$ which is defined by

$$c = C'^*(c')A'^*(c')^{-1}B'^*(c')^{-1}\ . \tag{5.4}$$

In other words, we have

$$\begin{aligned} &c(h_1, h_2, \ldots, h_n) = \\ &\qquad = c'(h_1+h_2, h_3, \ldots, h_n)c'(h_1, h_3, \ldots, h_n)^{-1}c'(h_2, h_3, \ldots, h_n)^{-1} \end{aligned} \tag{5.5}$$

for all points h_i, $1 \le i \le n$, of H. We now have to show that if c' satisfies (c0), (c1), (c2) of 3.b (ii) with n replaced by $n-1$, then c satisfies (c0), (c1), (c2) for n: It is clear that c satisfies (c0) and that c is symmetric in the "variables" h_1, h_2 and in $h_3, \ldots, h_n$ separately. To show that c satisfies (c1) in general, it is enough to show that, in addition, we have

$$c(h_1, h_2, h_3, \ldots, h_n) = c(h_1, h_3, h_2, \ldots, h_n). \tag{5.6}$$

To explain this we may assume that $n = 3$ (the argument for $n > 3$ is essentially the same). By the cocycle condition (c2) for c' we obtain: $c'(h_2 + h_1, h_3)c'(h_1, h_3)^{-1} = c'(h_2, h_1 + h_3)c'(h_2, h_1)^{-1}$. By multiplying both sides with $c'(h_2, h_3)^{-1}$ and using the symmetry condition for c' we obtain (5.6) and this shows condition (c1) for c. The cocycle condition (c2) for c now follows directly from (5.5). This proves the first statement of the Lemma. To show the second statement we first observe that our construction is functorial. The rest follows from the definition of the product of multiextensions. □

Lemma 5.2. *Suppose that $(\mathcal{L}, \xi)$ is an invertible sheaf with an n-cubic structure over H which is such that the corresponding $n-1$-extension $E(\mathcal{L}, \xi)$ of 5.a is trivial as a symmetric multiextension. Then there is an $n-1$-cubic structure ξ' on $\mathcal{L}$ which induces the n-cubic structure ξ by the procedure of Lemma 5.1. Conversely, if the n-cubic structure ξ is induced from an $n-1$-cubic structure ξ' by the procedure of Lemma 5.1 then $E(\mathcal{L}, \xi)$ is trivial as a symmetric multiextension.*

PROOF. (For $n = 3$ and general H this is essentially [Br] Prop. 2.11.) Suppose that $E(\mathcal{L}, \xi)$ is trivial as a symmetric $n-1$-extension. By definition, this means that there is an isomorphism

$$\xi' : \mathcal{O}_{H^{n-1}} \xrightarrow{\sim} E(\mathcal{L}, \xi) := \Theta_{n-1}(\mathcal{L})$$

which is compatible with the partial composition laws (4.4) and the symmetry isomorphisms

$$\mathfrak{P}_\tau : \tau^*\Theta_{n-1}(\mathcal{L}) \xrightarrow{\sim} \Theta_{n-1}(\mathcal{L})$$

for all $\tau \in S_{n-1}$. Recall that the composition laws on $E(\mathcal{L}, \xi)$ are given by (5.2). We can now see that the isomorphism ξ' is compatible with the composition law for $i = 1$ if and only if $\xi : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L})$ is obtained from the isomorphism ξ' by the procedure described in the beginning of 5.b. We just have to show that the isomorphism ξ' defines an $n-1$-cubic structure. For this purpose, we may assume that R is local and that $\mathcal{L}$ is the trivial invertible sheaf on H (see 3.b (ii)). As in the proof of the previous lemma, we see that the isomorphisms ξ, ξ' are given by elements $c \in R[G^n]^*$, $c' \in R[G^{n-1}]^*$ respectively which are related by (5.5). Since ξ is an n-cubic structure, c satisfies (c0), (c1) and (c2) of 3.b (ii). We would like to show that c' satisfies (c0), (c1) and (c2) with n replaced by $n-1$. Property (c0) follows immediately from (5.5). Since ξ' is compatible with the symmetry isomorphisms c' satisfies (c1). It remains to show property (c2); the relevant equation can be written

$$\begin{aligned} (5.7) \quad & c'(h_1 + h_2, h_3, \ldots, h_n)c'(h_2, h_3, \ldots, h_n)^{-1} = \\ & \qquad = c'(h_1, h_2 + h_3, \ldots, h_n)c'(h_1, h_2, \ldots, h_n)^{-1} . \end{aligned}$$

This now follows from Property (c1) for c and (5.5). We will leave the converse to the reader. □

Remark 5.3. Note that in the paragraph above we assumed that $n \geq 3$. Suppose now that $n = 2$. Then we have $\Theta_{n-1}(\mathcal{L}) = \Theta_1(\mathcal{L}) = \mathcal{L} \otimes 0^*\mathcal{L}^{-1}$. Hence, if $E(\mathcal{L}, \xi)$ is a trivial (1-)extension and $0^*\mathcal{L}$ a trivial invertible $\mathcal{O}_H$-sheaf then $\mathcal{L}$ is also a trivial invertible $\mathcal{O}_H$-sheaf.

5.c. Let $n \geq 1$. Suppose that $(\mathcal{L}, \xi)$ is an invertible sheaf with an $n+1$-cubic structure over H. If $\Delta_n : H \to H^n$ is the diagonal morphism, then we can consider the invertible sheaf $\delta(\mathcal{L}, \xi) := \Delta_n^*\Theta_n(\mathcal{L}) = \Delta_n^* E(\mathcal{L}, \xi)$ on H and set

$$\mathcal{L}^\flat := \delta(\mathcal{L}, \xi) \otimes \mathcal{L}^{\otimes -n!} . \tag{5.8}$$

Proposition 5.4. *Suppose that $n \geq 2$. Then the invertible sheaf $\mathcal{L}^\flat$ defined above is equipped with a canonical n-cubic structure $\xi^\flat$.*

Remark 5.5. Notice that the invertible sheaf $\delta(\mathcal{L}, \xi)$ is always "rigid", i.e equipped with an isomorphism $0^*\delta(\mathcal{L}, \xi) \simeq \mathcal{O}_H$. Hence, there is an isomorphism

$$0^*\mathcal{L}^\flat \simeq 0^*\mathcal{L}^{-\otimes n!}.$$

Also notice that when $n = 1$, we have $\mathcal{L}^\flat = \delta(\mathcal{L}, \xi) \otimes \mathcal{L}^{-1} = \Theta_1(\mathcal{L}) \otimes \mathcal{L}^{-1} = 0^*\mathcal{L}^{-1}$.

Notice that successive application of Proposition 5.4, combined with the above remark, gives the following. (See Remark 9.9 for an interpretation of a special case of this formula in the context of a Riemann-Roch theorem.)

Corollary 5.6. (Taylor expansion) *There is an isomorphism of invertible sheaves*

$$\mathcal{L}^{\otimes n!!} \simeq (0^*\mathcal{L})^{\otimes n!!} \otimes \bigotimes_{i=0}^{n-1} \delta(\mathcal{L}^{(i)}, \xi^{(i)})^{\otimes(-1)^i(n-i-1)!!} \tag{5.9}$$

where $(\mathcal{L}^{(0)}, \xi^{(0)}) := (\mathcal{L}, \xi)$, $(\mathcal{L}^{(i)}, \xi^{(i)}) := ((\mathcal{L}^{(i-1)})^\flat, (\xi^{(i-1)})^\flat)$ *and* $n!! = n!(n-1)!\cdots 2!$.

Proof of 5.4. For simplicity, we set $E = E(\mathcal{L}, \xi)$, $\delta = \delta(\mathcal{L}, \xi)$. If R' is an R-algebra we consider $H(R') = H(\mathrm{Spec}\,(R'))$; this is the group of characters of G with values in R'. Let $\chi_0, \chi_1, \ldots, \chi_n$ be R'-valued characters of G. If S is a subset of $\{0, \ldots, n\}$, we set $\chi_S = \prod_{i\in S} \chi_i$. (Here and below a product, resp. a tensor product, over the empty set is 1, resp. the trivial invertible sheaf.) By the definition, we have

$$\Theta_n(\delta)_{(\chi_1,\ldots,\chi_n)} = \bigotimes_{S\subset\{1,\ldots,n\}} E_{(\chi_S,\ldots,\chi_S)}{}^{(-1)^{n-\#S}}. \tag{5.10}$$

Repeated application of the composition laws (4.4) now provide functorial isomorphisms

$$\bigotimes_{p:\{1,\ldots,n\}\to S} E_{(\chi_{p(1)},\ldots,\chi_{p(n)})} \xrightarrow{\sim} E_{(\chi_S,\ldots,\chi_S)} \tag{5.11}$$

(the tensor product runs over all maps $p : \{1, \ldots, n\} \to S$). Observe that if $S \neq \{1, \ldots, n\}$ we have

$$\sum_{S';S\subset S'\subset\{1,\ldots,n\}} (-1)^{n-\#S'} = 0\ . \tag{5.12}$$

This shows that in the tensor product

$$\bigotimes_{S\subset\{1,\ldots,n\}} \bigotimes_{p:\{1,\ldots,n\}\to S} E_{(\chi_{p(1)},\ldots,\chi_{p(n)})}{}^{(-1)^{n-\#S}} \tag{5.13}$$

the terms for which either $S \neq \{1, \ldots, n\}$ or $S = \{1, \ldots, n\}$ and p is not surjective contract (canonically). Therefore, we are left with

$$\bigotimes_{p:\{1,\ldots,n\}\xrightarrow{\sim}\{1,\ldots,n\}} E_{(\chi_{p(1)},\ldots,\chi_{p(n)})}\ . \tag{5.14}$$

Hence, using the symmetry isomorphisms and (5.10) we can see that there is a canonical isomorphism

$$(E_{(\chi_1,\ldots,\chi_n)})^{\otimes n!} \xrightarrow{\sim} \Theta_n(\delta)_{(\chi_1,\ldots,\chi_n)}\ . \tag{5.15}$$

Since by definition $E = \Theta_n(\mathcal{L})$ we obtain from (5.15) a canonical isomorphism

$$\xi^\flat : \mathcal{O}_{H^n} \xrightarrow{\sim} \Theta_n(\mathcal{L}^\flat) = \Theta_n(\delta \otimes \mathcal{L}^{-\otimes n!}) \simeq \Theta_n(\delta) \otimes \Theta_n(\mathcal{L})^{-\otimes n!}\ . \tag{5.16}$$

We will now show that the isomorphism (5.16) above satisfies the conditions (c0), (c1), (c2) of an n-cubic structure. For this purpose, we may assume that R is local and that $\mathcal{L}$ is the trivial invertible sheaf on H (see 3.b (ii)-(iii)). Then all the invertible sheaves in the

construction above are also trivial and the hypercubic structure ξ is given by an $n+1$-cubic element $c \in R[G^{n+1}]^*$. By unraveling the definition above we can now see that the isomorphism (5.16) is given as multiplication by

$$\prod_{S\subset\{1,\ldots,n\}} (\chi_1\otimes\cdots\otimes\chi_n)(d_S)^{(-1)^{n-\#S}} \tag{5.17}$$

where $d_S \in R[G^n]^*$ and the term $(\chi_1\otimes\cdots\otimes\chi_n)(d_S)$ gives the isomorphism (5.11). (The element d_S gives the isomorphism (5.11) for χ_i, $i=1,\ldots,n$, the "universal" $R[G^n]$-valued characters $G\to G^n\subset R[G^n]$, given by $\chi_i(g)=(g_j)_j$, with $g_j=g$ if $j=i$, $g_j=1$

if $j\neq i$. Notice that if $\#S\leq 1$, then $d_S=1$.) In fact, it is more convenient to consider the inverse of (5.11) and view that as the composition of several isomorphisms in which the arguments χ_S are unraveled one by one. Suppose that $S=\{i_1<i_2<\cdots<i_m\}\neq\emptyset$. Then the first of these isomorphisms is

$$E_{(\chi_S,\ldots,\chi_S)} \xrightarrow{\sim} \bigotimes_{k=1}^{m} E_{(\chi_{i_k},\chi_S,\ldots,\chi_S)}\ . \tag{5.18}$$

By the definition of the composition law of the n-extension $E=E(\mathcal{L},\xi)$ (see 5.a), this is described by the inverse of the element:

$$\begin{aligned}
&(\chi_{i_1}\otimes\prod_{k>1}\chi_{i_k}\otimes\chi_S\otimes\ \cdots\ \otimes\chi_S)(c)\cdot\\
&\cdot(\chi_{i_2}\otimes\prod_{k>2}\chi_{i_k}\otimes\chi_S\otimes\ \cdots\ \otimes\chi_S)(c)\cdot\\
&\qquad\vdots\\
&\cdot(\chi_{i_{m-1}}\otimes\chi_{i_m}\otimes\chi_S\otimes\ \cdots\ \otimes\chi_S)(c).
\end{aligned}$$

Using 3.c we see that we can write this as the value of the element

$$\Big(\sum_{p=1}^{m-1}\{([\chi_{i_p}]-[1])\otimes([\prod_{k>p}\chi_{i_k}]-[1])\}\Big)\otimes([\chi_S]-[1])\otimes\cdots\otimes([\chi_S]-[1])$$

of $C_{n+1}(H(R'))$ at c^{-1}. For simplicity, we set

$$A_S=\sum_{k=1}^{m}([\chi_{i_k}]-[1])\ ,\quad B_S=\sum_{p=1}^{m-1}\{([\chi_{i_p}]-[1])\otimes([\prod_{k>p}\chi_{i_k}]-[1])\}\ . \tag{5.19}$$

Similarly, we can now see that the isomorphisms

$$E_{(\chi_{i_k},\chi_S\cdots,\chi_S)} \xrightarrow{\sim} \bigotimes_{p=1}^{m} E_{(\chi_{i_k},\chi_{i_p},\chi_S,\ldots,\chi_S)} \tag{5.20}$$

which give the next step in unraveling the inverse of (5.11) are described by evaluating at c^{-1} the element

$$([\chi_{i_k}]-[1])\otimes B_S\otimes([\chi_S]-[1])\otimes\cdots\otimes([\chi_S]-[1]). \tag{5.21}$$

The combined effect (for $k = 1, \cdots, m$) of all of these on the tensor product of (5.18) is given by evaluating at c^{-1} the element

$$A_S \otimes B_S \otimes (([\chi_S] - [1]))^{\otimes(n-2)} \ . \tag{5.22}$$

The next step is unraveling the first remaining χ_S in $E_{(\chi_{i_k}, \chi_{i_p}, \chi_S, \ldots, \chi_S)}$. As above, we can see that this is given by the elements

$$([\chi_{i_k}] - [1]) \otimes ([\chi_{i_p}] - [1]) \otimes B_S \otimes ([\chi_S] - [1])^{\otimes(n-3)} \tag{5.23}$$

with combined effect

$$A_S^{\otimes 2} \otimes B_S \otimes ([\chi_S] - [1])^{\otimes(n-3)} \tag{5.24}$$

and so on. Putting everything together we see that $(\chi_1 \otimes \cdots \otimes \chi_n)(d_S)$ is given by evaluating the element

$$\Psi_S(\chi_1, \cdots, \chi_n) = \sum_{j=0}^{n-1} A_S^{\otimes j} \otimes B_S \otimes ([\chi_S] - [1])^{\otimes(n-j-1)} \tag{5.25}$$

of $C_{n+1}(H(R'))$ at c. Hence, the isomorphism (5.16) is given by an element $d \in R[G^n]^*$ which is such that

$$(\chi_1 \otimes \cdots \otimes \chi_n)(d) = \Bigg(\sum_{\substack{S \subset \{1,\ldots,n\} \\ S \neq \emptyset}} (-1)^{n-\#S} \Psi_S(\chi_1, \ldots, \chi_n) \Bigg)(c) \ . \tag{5.26}$$

For simplicity, set

$$\Phi(\chi_1, \ldots, \chi_n) = \sum_{S \subset \{1,\ldots,n\}} (-1)^{n-\#S} \Psi_S(\chi_1, \ldots, \chi_n) \tag{5.27}$$

in $C_{n+1}(H(R'))$ (here by definition $\Psi_\emptyset = 0$). The proof of the proposition will follow if we show the following properties:

f0) $\Phi(1, \ldots, 1) = 0$,

f1) $\Phi(\chi_{\sigma(1)}, \ldots, \chi_{\sigma(n)}) = \Phi(\chi_1, \ldots, \chi_n)$, for all $\sigma \in S_n$,

f2)
$$\begin{aligned} &\Phi(\chi_0\chi_1, \chi_2, \ldots, \chi_n) + \Phi(\chi_0, \chi_1, \chi_3, \ldots, \chi_n) = \\ &\qquad = \Phi(\chi_0, \chi_1\chi_2, \chi_3, \ldots, \chi_n) + \Phi(\chi_1, \chi_2, \ldots, \chi_n). \end{aligned}$$

Property (f0) is obvious and it is enough to concentrate on (f1) and (f2). Let $F = \{\prod_{i=0}^n x_i^{k_i} \mid k_i \in \mathbf{Z}\}$ be the free abelian group generated by the symbols $x_0, x_1, \ldots, x_n$ and let us consider $C_k(F) := \mathrm{Sym}^k_{\mathbf{Z}[F]} I[F]$, for $k \geq 1$. Recall that we denote by $I[F]^k$ the k-th power of the augmentation ideal $I[F]$ of the group ring $\mathbf{Z}[F]$.

Lemma 5.7. *The multiplication morphism $a_1 \otimes \cdots \otimes a_k \mapsto a_1 \cdots a_k$ induces an isomorphism*

$$C_k(F) = \mathrm{Sym}^k_{\mathbf{Z}[F]} I[F] \xrightarrow{\sim} I[F]^k \subset \mathbf{Z}[F].$$

Proof. In this case, $\mathbf{Z}[F] \simeq \mathbf{Z}[u_0, u_0^{-1}, \ldots, u_n, u_n^{-1}]$ (the ring of Laurent polynomials in $n+1$ indeterminants) with $I[F]$ corresponding to the ideal $(u_0 - 1, \ldots, u_n - 1)$. Consider the ideal $I = (v_0, \ldots, v_n)$ in the polynomial ring $\mathbf{Z}[\underline{v}] := \mathbf{Z}[v_0, \ldots, v_n]$. Multiplication $\mathrm{Sym}^k_{\mathbf{Z}[\underline{v}]} I \to I^k$ gives an isomorphism and the desired statement follows from this fact by setting $v_i = u_i - 1$ and localizing. $\square$

Suppose that y_i, $1 \leq i \leq n$, are elements of F. The identities (5.25), (5.27) with χ_i replaced by y_i can be used to define elements $\Psi_S(y_1, \ldots, y_n)$, $\Phi(y_1, \ldots, y_n) \in C_{n+1}(F)$. The group homomorphism $F \to H(R')$ given by $x_i \mapsto \chi_i$ induces a homomorphism $C_{n+1}(F) \to C_{n+1}(H(R'))$ which sends the elements $\Phi(x_1, \ldots, x_n)$, $\Phi(x_0x_1, \ldots, x_n)$, to $\Phi(\chi_1, \ldots, \chi_n)$, $\Phi(\chi_0\chi_1, \ldots, \chi_n)$ etc. Hence, it is enough to show

$$\begin{aligned}
&\text{g1)} \qquad \Phi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \Phi(x_1, \ldots, x_n), \text{ for all } \sigma \in S_n, \\
&\text{g2)} \qquad \Phi(x_0x_1, x_2, \ldots, x_n) + \Phi(x_0, x_1, x_3, \ldots, x_n) = \\
&\qquad\qquad = \Phi(x_0, x_1x_2, x_3, \ldots, x_n) + \Phi(x_1, x_2, \ldots, x_n).
\end{aligned}$$

In what follows, we will identify $C_k(F)$ with $I[F]^k$ using the multiplication morphism of Lemma 5.7. Furthermore, we will eliminate the brackets from the notation of elements of the group ring $\mathbf{Z}[F]$.

As above, if $S = \{i_1 < \cdots < i_m\} \subset \{1, \ldots, n\}$, we set

$$\begin{aligned}
A_S &= A_S(y_1, \ldots, y_n) = \sum_{k=1}^{m} y_{i_k} - m, \\
B_S &= B_S(y_1, \ldots, y_n) = \sum_{p=1}^{m-1} \{(y_{i_p} - 1)(\prod_{k>p} y_{i_k} - 1)\},
\end{aligned} \tag{5.28}$$

and also

$$P_S = P_S(y_1, \ldots, y_n) = \prod_{k=1}^{m} y_{i_k} - 1 \ . \tag{5.29}$$

Lemma 5.8. $\Psi_S(y_1, \ldots, y_n) = P_S^n - A_S^n$.

Proof. By the definition of $\Psi_S(y_1, \ldots, y_n)$ we have

$$\Psi_S(\chi_1, \cdots, \chi_n) = \sum_{j=0}^{n-1} A_S^j B_S P_S^{n-j-1} = B_S \cdot (\sum_{j=0}^{n-1} A_S^j P_S^{n-j-1}). \tag{5.30}$$

However, observe that by telescoping we find

$$\begin{aligned}
B_S(y_1, \ldots, y_n) &= \sum_{p=1}^{m-1} \{(y_{i_p} - 1)(\prod_{k>p} y_{i_k} - 1)\} = \\
&= (\prod_{k=1}^{m} y_{i_k} - 1) - (\sum_{k=1}^{m} y_{i_k} - m) = P_S - A_S.
\end{aligned} \tag{5.31}$$

The result now follows from the standard identity. $\square$

Lemma 5.8 and the definition of $\Phi(y_1, \dots, y_n)$ (cf. (5.27)) now imply

$$\Phi(y_1, \dots, y_n) = \sum_{S \subset \{1,\dots,n\}} (-1)^{n-\#S}((\prod_{i \in S} y_i - 1)^n - (\sum_{i \in S} y_i - \#S)^n) \ . \tag{5.32}$$

Notice that (g1) now follows immediately. It remains to show (g2). To do that we will compare terms between the two sides of the equation (g2). Let us consider the left hand side of the equation. Using (5.32) above we can see that it is a sum:

$$Z + Y(x_0x_1, x_2, \dots, x_n) + Y(x_0, x_1, x_3, \dots, x_n),$$

where we set

$$Y(y_1, \dots, y_n) = -\sum_{S \subset \{1,\dots,n\}} (-1)^{n-\#S}(\sum_{i \in S}(y_i - 1))^n \ ,$$

and where Z is a sum of terms which are either of the form $(-1)^{n-(\#T-1)}(\prod_{i \in T} x_i - 1)^n$ or of the form $(-1)^{n-\#T}(\prod_{i \in T} x_i - 1)^n$, for certain $T \subset \{0, 1, \dots, n\}$. More specifically, we can write

$$Z = 2\Sigma_1 + \Sigma_2 + \Sigma_3.$$

where

$$\Sigma_1 = \sum_{\{0,1,2\} \cap T = \emptyset} (-1)^{n-\#T}(\prod_{i \in T} x_i - 1)^n,$$

$$\Sigma_2 = \sum_{\{0,1,2\} \subset T} (-1)^{n-(\#T-1)}(\prod_{i \in T} x_i - 1)^n,$$

$$\Sigma_3 = \sum_{\#(T \cap \{0,1,2\})=1} (-1)^{n-\#T}(\prod_{i \in T} x_i - 1)^n.$$

(In these sums, T ranges over subsets of $\{0, 1, \dots, n\}$.) The rest of the terms cancel out since they appear twice but with different signs in $\Phi(x_0x_1, x_2, \dots, x_n)$ and $\Phi(x_0, x_1, \dots, x_n)$.

Similarly, a careful look at the right hand side of (g2) reveals that it is equal to the sum

$$Z + Y(x_0, x_1x_2, x_3, \dots, x_n) + Y(x_1, x_2, \dots, x_n) \ .$$

Now observe that the identity

$$\sum_{S \subset \{1,\dots,n\}} (-1)^{n-\#S}(\sum_{i \in S} z_i)^n = n! z_1 z_2 \cdots z_n$$

gives

$$Y(y_1, \dots, y_n) = -n! \prod_{k=1}^{n} (y_i - 1) \ .$$

Hence, by the above, we can now conclude that (g2) is equivalent to the identity

$$\begin{aligned} (x_0x_1 - 1)(x_2 - 1) \cdots (x_n - 1) + (x_0 - 1)(x_1 - 1) \cdots (x_n - 1) = \\ = (x_0 - 1)(x_1x_2 - 1) \cdots (x_n - 1) + (x_1 - 1)(x_2 - 1) \cdots (x_n - 1) \ , \end{aligned} \tag{5.33}$$

which is easily seen to be true. This concludes the proof of the identity (g2) and of Proposition 5.4. ☐

6. Multiextensions and abelian sheaves

In the next few paragraphs, we will not distinguish in our notation between a commutative group scheme A over a scheme T and the sheaf of abelian groups on the site $T_{\rm fppf}$ which is given by the sections of A. We will use the derived category of the homotopy category of complexes of sheaves of abelian groups on $T_{\rm fppf}$ (recall that $T_{\rm fppf}$ is the site of T-schemes which are locally of finite presentation with the fppf topology). Otherwise, we continue with the notations and general set-up of §4. If $Y \to S$ is an object of $S_{\rm fppf}$, we will denote by $\mathbf{Z}[Y]$ the abelian sheaf on the fppf site of S which is freely generated by the points of Y (see [SGA4] IV 11). If Y and Y' are two objects of $S_{\rm fppf}$ then there is a canonical isomorphism:

$$\mathbf{Z}[Y] \overset{\rm L}{\otimes} \mathbf{Z}[Y'] = \mathbf{Z}[Y] \otimes \mathbf{Z}[Y'] \simeq \mathbf{Z}[Y \times_S Y']. \tag{6.1}$$

The natural morphism of sheaves $Y \to \mathbf{Z}[Y]$ induces a canonical isomorphism ([SGA7I] VII 1.4):

$$\mathrm{Ext}^1(\mathbf{Z}[Y], J) \xrightarrow{\sim} \mathrm{H}^1(Y, J_Y). \tag{6.2}$$

Now suppose that $H \to S$ is a commutative group scheme which is finite locally free over S. We will denote by $\epsilon_H : \mathbf{Z}[H] \to H$ the augmentation homomorphism. Then, under 6.2, the homomorphism $\mathrm{Ext}^1(\epsilon_H, J)$ is identified with the natural homomorphism

$$\mathrm{Ext}^1(H, J) \to \mathrm{H}^1(H, J). \tag{6.3}$$

Suppose F, F' are abelian sheaves (on $S_{\rm fppf}$) and E a complex of abelian sheaves which is bounded above. Then there is a canonical spectral sequence

$$\mathrm{Ext}^p(E, \underline{\mathrm{Ext}}^q(F, F')) \Rightarrow \mathrm{Ext}^{p+q}(E, \underline{\mathbf{R}\mathrm{Hom}}(F, F')) \tag{6.4}$$

which induces an exact sequence:

$$0 \to \mathrm{Ext}^1(E, \underline{\mathrm{Hom}}(F, F')) \to \mathrm{Ext}^1(E, \underline{\mathbf{R}\mathrm{Hom}}(F, F')) \to \mathrm{Ext}^1(E, \underline{\mathrm{Ext}}^1(F, F')). \tag{6.5}$$

There is also a canonical isomorphism:

$$\mathrm{Ext}^p(E, \underline{\mathbf{R}\mathrm{Hom}}(F, F')) \xrightarrow{\sim} \mathrm{Ext}^p(E \overset{\rm L}{\otimes} F, F'). \tag{6.6}$$

6.a. By [SGA7I] VII (2.5.4.1) and 3.6.7 (see also loc. cit. 3.6.4, 3.6.5 and the remarks in VIII §0.2) there are canonical isomorphisms

$$n\text{-}\mathrm{Ext}^0(H, J) \xrightarrow{\sim} \mathrm{Hom}(\underbrace{H \otimes \cdots \otimes H}_{n}, J)\ , \tag{6.7}$$

$$n\text{-}\mathrm{Ext}^1(H, J) \xrightarrow{\sim} \mathrm{Ext}^1(\underbrace{H \overset{\rm L}{\otimes} \cdots \overset{\rm L}{\otimes} H}_{n}, J)\ . \tag{6.8}$$

In the source of the second morphism $H \overset{\mathrm{L}}{\otimes} \cdots \overset{\mathrm{L}}{\otimes} H = ((H \overset{\mathrm{L}}{\otimes} \cdots \overset{\mathrm{L}}{\otimes} H) \overset{\mathrm{L}}{\otimes} H) \overset{\mathrm{L}}{\otimes} H$ is the complex, well-defined up to canonical isomorphism in the derived category, obtained by applying successively the derived tensor product functor.

When $J = \mathbf{G}_m$, the discussion in loc. cit. shows that the diagram

$$\begin{array}{ccc} n\text{-}\mathrm{Ext}^1(H, \mathbf{G}_m) & \xrightarrow{\sim} & \mathrm{Ext}^1(H \overset{\mathrm{L}}{\otimes} \cdots \overset{\mathrm{L}}{\otimes} H, \mathbf{G}_m) \\ \downarrow t & & \downarrow \\ \mathrm{Pic}(H \times_S \cdots \times_S H) & \xrightarrow{\sim} & \mathrm{Ext}^1(\mathbf{Z}[H] \otimes \cdots \otimes \mathbf{Z}[H], \mathbf{G}_m) \end{array} \tag{6.9}$$

commutes. Here the second vertical isomorphism is $\mathrm{Ext}^1(\epsilon_H \overset{\mathrm{L}}{\otimes} \cdots \overset{\mathrm{L}}{\otimes} \epsilon_H, \mathbf{G}_m)$, and the lower horizontal isomorphism is given by (6.2) and (6.1).

6.b. We continue to assume that $H \to S$ is finite locally free. Once again, we denote by $H^D = \underline{\mathrm{Hom}}(H, \mathbf{G}_m)$ the Cartier dual of H; let $\{\ ,\ \} : H^D \times H \to \mathbf{G}_m$ be the natural pairing. By [SGA7I] VIII Prop. 3.3.1, $\underline{\mathrm{Ext}}^1(H^D, \mathbf{G}_m) = (0)$. Then, the exact sequence (6.5) gives an isomorphism

$$\mathrm{Ext}^1(E, H^D) \xrightarrow{\sim} \mathrm{Ext}^1(E, \mathbf{R}\underline{\mathrm{Hom}}(H, \mathbf{G}_m)). \tag{6.10}$$

By composing (6.8) with (6.10) and (6.6) we obtain a canonical isomorphism

$$\mathrm{Ext}^1(\underbrace{H \otimes^{\mathrm{L}} \cdots \otimes^{\mathrm{L}} H}_{n-1}, H^D) \xrightarrow{\sim} n\text{-}\mathrm{Ext}^1(H, \mathbf{G}_m), \tag{6.11}$$

hence also

$$(n-1)\text{-}\mathrm{Ext}^1(H, H^D) \xrightarrow{\sim} n\text{-}\mathrm{Ext}^1(H, \mathbf{G}_m). \tag{6.12}$$

For $n = 1$, (6.11) amounts to an isomorphism

$$\mathrm{H}^1(S, H^D) \simeq \mathrm{Ext}^1(\mathbf{Z}, H^D) \xrightarrow{\sim} \mathrm{Ext}^1(H, \mathbf{G}_m). \tag{6.13}$$

To describe this last isomorphism explicitly, suppose we start with an H^D-torsor $Q \to S$ which, under (6.2), corresponds to the extension

$$0 \to H^D \to Q' \to \mathbf{Z} \to 0.$$

Tensoring with H gives an extension

$$0 \to H^D \otimes H \to Q' \otimes H \to H \to 0$$

which we can push out by $H^D \otimes H \to \mathbf{G}_m; a \otimes h \mapsto \{a, h\}$, to obtain an extension of H by $\mathbf{G}_m$. We can see that this push-out extension is isomorphic to

$$1 \to \mathbf{G}_m \to (Q \times_S H \times_S \mathbf{G}_m)/H^D \to H \to 0\,. \tag{6.14}$$

Here the (representable) fppf sheaf in the middle is the quotient sheaf for the action of H^D on $Q \times_S H \times_S \mathbf{G}_m$ given by $(q, h, u) \cdot a = (q \cdot a, h, \{a, h\}^{-1} u)$ and has group structure given via descent by $(q, h, u) \cdot (q', h', u') = (q, hh', \{q^{-1}q', h'\} uu')$. The isomorphism (6.13) and the explicit extension (6.14) are discussed in detail in [Wa]; see Theorems 2 and 3. When H^D is constant, then loc. cit. Theorem 3 implies that the extension (6.14) is the negative

of the extension (2.13) which was associated to the H^D-torsor Q in §2.b; cf. Remark 6.2 (b) below.

In fact, we can obtain a similar description for the map (6.12) (cf. [SGA7I] VIII (1.1.6) where the details of this construction for $n = 2$ are left to the reader): Suppose that $Q \to H^{n-1}$ is the $H^D_{H^{n-1}}$-torsor supporting the structure of an $n-1$-extension of H by H^D. The construction (6.14) applied to $S = H^{n-1}$ provides us with an extension of $H_{H^{n-1}}$ by $\mathbf{G}_{mH^{n-1}}$. The underlying $\mathbf{G}_{mH^n}$-torsor over $H_{H^{n-1}} = H^n$ then supports a canonical structure of n-extension whose isomorphism class is the image of the class of Q under the map (6.12).

6.c. We continue to assume that $H \to S$ is finite locally free. For future use we observe that the following diagram is commutative:

$$\begin{array}{ccccc} n\text{-Ext}^1(H,\mathbf{G}_m) & \xrightarrow{t} & \mathrm{Pic}(H^n) & \xrightarrow{\Delta_n^*} & \mathrm{Pic}(H) \\ {\scriptstyle(6.12)}\uparrow\wr & & & & \uparrow\Delta_2^* \\ (n-1)\text{-Ext}^1(H,H^D) & & & & \mathrm{Pic}(H\times H) \\ {\scriptstyle(4.7)}\downarrow t & & & & \uparrow t \\ \mathrm{H}^1(H^{n-1},H^D) & \xrightarrow{\Delta_{n-1}^*} & \mathrm{H}^1(H,H^D) & \xrightarrow[\sim]{(6.13)} & \mathrm{Ext}^1(H_H,\mathbf{G}_{mH}). \end{array} \tag{6.15}$$

This follows from the description of the maps (6.12), (6.13) in the previous paragraph.

6.d. Suppose now that $S = \mathrm{Spec}\,(R)$ and $H = G_S^D = \mathrm{Spec}\,(R[G])$ is the Cartier dual of the finite constant abelian group scheme G_S. Let $T \to S$ be an S-scheme; Suppose $q : Q \to T$ is a G-torsor; the construction (6.14) gives a corresponding extension of G_T^D by $\mathbf{G}_{mT}$. Suppose that $S' = \mathrm{Spec}\,(R') \to S$ is another S-scheme and consider a character $\chi : G \to R'^*$; this corresponds to a point $S' \to G_S^D$ which we will still denote by χ. Now suppose that T' is an $S' \times_S T$-scheme and consider the morphism $f : T' \to S' \times_S T \xrightarrow{(\chi,\mathrm{id})} G_T^D = G_S^D \times_S T$. By pulling back the $\mathbf{G}_{mT}$-torsor underlying the extension (6.14) along $f : T' \to G_T^D$ we obtain a $\mathbf{G}_{mT'}$-torsor (i.e an invertible sheaf) $\mathcal{L}_f^Q$ over T'. By definition, the class of $\mathcal{L}_f^Q$ is the image of the class of Q under the composition

$$\mathrm{H}^1(T,G) \xrightarrow{(6.13)} \mathrm{Ext}^1(G_T^D,\mathbf{G}_{mT}) \to \mathrm{Pic}(G_T^D) \xrightarrow{f^*} \mathrm{Pic}(T'). \tag{6.16}$$

Now recall (§2.d) that $q_*(\mathcal{O}_Q)$ is actually a coherent sheaf of $\mathcal{O}_T[G] = \mathcal{O}_T \otimes_R R[G]$-modules; we may think of it as a coherent $\mathcal{O}_{G_T^D}$-module which by (2.7) is invertible.

Lemma 6.1. *Let G act on $q_*(\mathcal{O}_Q) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'}$ via $g \cdot (b \otimes t') = g \cdot b \otimes \chi(g)t'$. The sheaf of invariants $(q_*(\mathcal{O}_Q) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'})^G$ is an invertible sheaf of $\mathcal{O}_{T'}$-modules and we have*

$$\mathcal{L}_f^Q \simeq (q_*(\mathcal{O}_Q) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'})^G.$$

Proof. This is a special case of [Wa] Theorem 3. It also follows directly from the explicit description of the middle sheaf in the extension 6.14 as a quotient and the fact that in this case of free G-action taking quotient commutes with base change (see (2.1)). □

Remark 6.2. a) Suppose that we take $T' = S' \times_S T$ and $f = (\chi, \mathrm{id})$. For simplicity, we set $\mathcal{L}^Q_\chi := \mathcal{L}^Q_{(\chi,\mathrm{id})}$. Then, Lemma 6.1 implies that

$$\mathcal{L}^Q_\chi \simeq \mathcal{O}_{Q,\chi^{-1}} \tag{6.17}$$

with the right hand side defined in §2.d.

b) Recall the description of commutative extensions given in 4.a. Consider the points $(\chi, \mathrm{id}) : S' \to G^D_T$ given by S'-valued characters $\chi : G \to \mathcal{O}^*_{S'}$ as in (a) above. By 4.a, and the definition of $\mathcal{L}^Q_\chi$, there are functorial isomorphisms

$$\mathcal{L}^Q_\chi \otimes_{\mathcal{O}_{S'}} \mathcal{L}^Q_{\chi'} \xrightarrow{\sim} \mathcal{L}^Q_{\chi\chi'} \tag{6.18}$$

for any pair of characters χ, χ'. Theorem 3 of [Wa] implies that (6.17) takes the isomorphisms (6.18) above to the isomorphisms (2.9) defined in §2.d using the multiplication of $\mathcal{O}_Q$. In other words, (6.17) is actually obtained from an isomorphism between the extension (6.14) and the negative of the extension (2.13); we are not going to need this more precise statement.

7. Multiextensions of finite multiplicative group schemes

Suppose that $S = \mathrm{Spec}\,(\mathbf{Z})$ and $H = G^D$, the Cartier dual of a finite abelian *constant* group scheme G. If $G \simeq \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$, then

$$H \simeq \mu_{n_1} \times \cdots \times \mu_{n_r} \tag{7.1}$$

where $\mu_k = \mathrm{Spec}\,(\mathbf{Z}[x]/(x^k - 1))$ denotes the group scheme of k-th roots of unity over $\mathbf{Z}$. Our goal in this section is to understand the category of n-extensions of H by $\mathbf{G}_m$. The main result is Theorem 7.8.

7.a. Let us suppose that $n \geq 2$.

Lemma 7.1. *With the above notations and assumptions*

$$n\text{-}\mathrm{Ext}^0(H, \mathbf{G}_m) = (\mathrm{id})\ .$$

Proof. We have ($n \geq 2$)

$$\mathrm{Hom}(\underbrace{H \otimes \cdots \otimes H}_{n}, \mathbf{G}_m) \simeq \mathrm{Hom}(\underbrace{H \otimes \cdots \otimes H}_{n-1}, H^D)\ .$$

Each element of this last group is given by a morphism $H^{n-1} = H \times_S \cdots_S \times H \to H^D$. Since H^{n-1} is connected and $H^D \simeq G$ is constant any such morphism factors through the identity section; hence this group is trivial. The result now follows from (6.7). □

Remark 7.2. a) Lemma 7.1 shows that for $n \geq 2$ the Picard category of n-extensions of H by $\mathbf{G}_m$ is "discrete", i.e there is at most one isomorphism between any two objects.

b) As a consequence of (a), any two symmetric n-extensions of H by $\mathbf{G}_m$ which are isomorphic as n-extensions are also isomorphic as *symmetric* n-extensions. Indeed, by (a), the diagram (4.9) of isomorphisms of n-extensions automatically commutes. In particular, if an n-extension of H by $\mathbf{G}_m$ is trivial as an n-extension then it is also trivial as a symmetric n-extension.

7.b. In what follows we will study the group $n\text{-}\mathrm{Ext}^1(H, \mathbf{G}_m)$ of isomorphism classes of n-extensions of $H = G^D$ by $\mathbf{G}_m$. We begin by introducing some notations.

If C is an abelian group and $m \geq 1$ an integer, we will denote by C/m, resp. ${}_mC$, the cokernel, resp. kernel, of the map $C \to C$ given by multiplication by m. Set $\zeta_r = e^{2\pi i/r}$ and for simplicity denote by $C(r)$ the ideal class group $\mathrm{Cl}(\mathbf{Q}(\zeta_r))$ of the cyclotomic field $\mathbf{Q}(\zeta_r)$. We will identify $(\mathbf{Z}/r\mathbf{Z})^*$ with the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_r)/\mathbf{Q})$ by sending $a \in (\mathbf{Z}/r\mathbf{Z})^*$ to σ_a defined by $\sigma_a(\zeta_r) = \zeta_r^a$. Now let p be a prime number; we will denote by v_p, resp. $|\ |_p$ the usual p-adic valuation, resp. p-adic absolute value. Consider the Teichmuller character $\omega : (\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}_p^*$ characterized by $a = \omega(a) \bmod p\mathbf{Z}_p$. For simplicity, set $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. We will view Δ as a direct factor of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^k})/\mathbf{Q})$ for any $k \geq 1$. Suppose D is a $\mathbf{Z}[\Delta]$-module which is annihilated by a power of p. For $i \in \mathbf{Z}$ we set

$$D^{(i)} = \{d \in D \mid \sigma_a(d) = \omega^i(a)d, \text{ for all } a \in (\mathbf{Z}/p\mathbf{Z})^*\}.$$

We have

$$D = \bigoplus_{0 \leq i \leq p-2} D^{(i)}.$$

We will consider the groups $\mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$, $k \geq 1$; these are naturally $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^k})/\mathbf{Q})$-modules via

$$(\sigma_a(\phi))(c) = \phi(\sigma_a^{-1}(c)) \quad \text{for } \phi : C(p^k) \to p^{-k}\mathbf{Z}/\mathbf{Z}. \tag{7.2}$$

Note that the norm $C(p^k) \to C(p^{k-1})$ for the extension $\mathbf{Q}(\zeta_{p^k})/\mathbf{Q}(\zeta_{p^{k-1}})$ induces a homomorphism

$$N_{k-1} : \mathrm{Hom}(C(p^{k-1}), p^{-(k-1)}\mathbf{Z}/\mathbf{Z}) \to \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \ .$$

Definition 7.3. *For $n \geq 1$, $m \geq 1$, let $\mathcal{C}(n; p^m)$ be the group of m-tuples*

$$(f_k)_{1 \leq k \leq m} \ ; \quad f_k \in \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$$

which satisfy

$$\begin{aligned} &i) & \sigma_a(f_k) &= a^{n-1} f_k, \text{ for all } a \in (\mathbf{Z}/p^k)^*, \\ &ii) & N_{k-1}(f_{k-1}) &= p^{n-1} f_k \ . \end{aligned}$$

Remark 7.4. Property (i) implies that

$$\mathcal{C}(n;p^m) \subset \bigoplus_{1\le k\le m} \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})^{(n-1)} =$$
$$= \bigoplus_{1\le k\le m} \mathrm{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z}).$$

In particular, since $(C(p^k)/p^k)^{(0)} = (0)$ we obtain $\mathcal{C}(1;p^m) = (0)$.

One of the main results in this section is:

Proposition 7.5. *There is a natural injective homomorphism*

$$\psi_n : n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) \to \bigoplus_{1\le k\le m} \mathrm{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z})$$

with image the subgroup $\mathcal{C}(n;p^m)$*.*

Before we consider the proof we will discuss some consequences of this result.

Corollary 7.6. *If* p *is a regular prime, then* $n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) = (0)$*.*

Now observe that $\mathcal{C}(n;p) \simeq \mathrm{Hom}(C(p), \mathbf{Z}/p)^{(n-1)}$. Hence, for $m = 1$ the result amounts to:

Corollary 7.7. *There are natural isomorphisms*

$$n\text{-}\mathrm{Ext}^1(\mu_p, \mathbf{G}_m) \xrightarrow{\sim} \mathrm{Hom}(C(p), \mathbf{Z}/p)^{(n-1)} \simeq \mathrm{Hom}((C(p)/p)^{(1-n)}, \mathbf{Z}/p)\ .$$

Recall that the k-th Bernoulli number B_k is defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}\ .$$

Also, recall that by [Bo], the Quillen K-groups $\mathrm{K}_m(\mathbf{Z})$ are finite for even integers $m \ge 2$. We set $h_p^+ = \#\mathrm{Cl}(\mathbf{Q}(\zeta_p + \zeta_p^{-1}))$ and

$$e(n) = \begin{cases} 1 & \text{, if } n = 1, \\ \text{numerator}\,(B_n/n) & \text{, if } n \text{ is even,} \\ \prod_{p, p \mid h_p^+} \mathrm{ord}_p(\#\mathrm{K}_{2n-2}(\mathbf{Z})) & \text{, if } n > 1 \text{ is odd.} \end{cases}$$

As we shall now see, Corollary 7.7 can now be used to obtain:

Theorem 7.8. *For every finite abelian group* G*, the group of isomorphism classes of* n*-extensions* $n\text{-}\mathrm{Ext}^1(G^D, \mathbf{G}_m)$ *is annihilated by*

$$\prod_{p \mid e(n)} \mathrm{ord}_p(\#G).$$

In particular, if $(\#G, e(n)) = 1$*, then* $n\text{-}\mathrm{Ext}^1(G^D, \mathbf{G}_m) = (0)$*.*

PROOF. Using (6.8) we can see that the group $n\text{-Ext}^1(G^D, \mathbf{G}_m)$ is annihilated by the order $\#G$ and that it can be written as direct sum

$$\bigoplus_{p|\#G} n\text{-Ext}^1(G_p^D, \mathbf{G}_m)$$

where G_p is the p-Sylow subgroup of G. The desired result will now follow if we show that $p \nmid e(n)$ implies $n\text{-Ext}^1(G_p^D, \mathbf{G}_m) = (0)$. Using (6.8) again and employing the long exact cohomology sequence which is obtained by unraveling G_p^D into its "simple pieces" (each isomorphic to μ_p) we see that it is enough to show that $p \nmid e(n)$ implies that $n\text{-Ext}^1(\mu_p, \mathbf{G}_m) = (0)$. Corollary 7.7 then implies that it suffices to show that when $p \nmid e(n)$, we have $(C(p)/p)^{(1-n)} = (0)$. This now follows from well-known results on cyclotomic ideal class groups ([W], [Ku], [So]). For the convenience of the reader we sketch the argument (we can assume that p is odd). First of all, when $n \geq 2$ is even the result follows directly from Herbrand's theorem ([W] Theorem 6.17) and Kummer's congruences ([W] Cor. 5.14 and Cor. 5.15). To deal with the case that n is odd, we will use the cohomology groups $\mathrm{H}^i(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) := \varprojlim_m \mathrm{H}^2_{\text{et}}(\mathbf{Z}[1/p], \mu_{p^m}^{\otimes n})$. By [Ku] Lemma 1.2 we have

$$\mathrm{H}^2(\mathbf{Z}[1/p], \mu_p^{\otimes n}) \simeq (C(p)/p)^{1-n},$$

while since $\mathrm{H}^3(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) = (0)$ we can see that

$$\mathrm{H}^2(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p \simeq \mathrm{H}^2(\mathbf{Z}[1/p], \mu_p^{\otimes n}).$$

(See [So], [Ku] for more details.) For $n \geq 2$, there is a surjective Chern character ([DF]; see [So])

$$\mathrm{ch} : \mathrm{K}_{2n-2}(\mathbf{Z}) \to \mathrm{H}^2(\mathbf{Z}[1/p], \mathbf{Z}_p(n)) \ .$$

Since $(C(p)/p)^{(0)} = (0)$ and $p \nmid h_p^+$ implies that $(C(p)/p)^{(1-n)} = (0)$ for $n > 1$ odd, these facts imply the result. $\square$

Remark 7.9. a) We have $B_2 = 1/6$, $B_4 = -1/30$ and $\mathrm{K}_4(\mathbf{Z})$ is trivial (see [Ro]; in fact, for our purposes it suffices to know that $\mathrm{K}_4(\mathbf{Z})$ has at most 6-power torsion. This is somewhat simpler and is shown in Soulé's addendum to [LS]). Hence, we see that Theorem 7.8 implies that for all finite abelian groups G

$$n\text{-Ext}^1(G^D, \mathbf{G}_m) = (0), \text{ for } n = 1, 2, 3, 4.$$

b) Note that [So] gives a doubly exponential bound on the size of $e(n)$ for n odd. However, according to the Kummer-Vandiver conjecture, $p \nmid h_p^+$. Assuming this we could replace in the statement of Theorem 7.8 $e(n)$ by $e'(n)$ given by $e'(n) = e(n)$ if n is even, $e'(n) = 1$ if n is odd. Actually when the prime divisors of $\#G$ satisfy the Kummer-Vandiver conjecture (which is true for all primes $< 12 \cdot 10^6$ by the computations of [BCEM]) we have

$$n\text{-Ext}^1(G^D, \mathbf{G}_m) = (0), \text{ for } 1 \leq n \leq 11.$$

Indeed, the first $e'(n)$ which is not equal to 1 is $e'(12) = 691$.

c) Note that the Quillen-Lichtenbaum conjecture, coupled with the argument in the proof of Theorem 7.8 above, implies that for $n > 1$ odd we have $e(n) = 2^a \cdot \#\mathrm{K}_{2n-2}(\mathbf{Z})$ $(a \in \mathbf{Z})$.

Before we continue, we observe that Theorem 7.8 together with the results of the previous section imply:

Theorem 7.10. *Let G be a finite abelian group and $n \geq 1$. If $\mathcal{L}$ is an invertible sheaf on $H = G^D_{\mathrm{Spec}\,(\mathbf{Z})} = \mathrm{Spec}\,(\mathbf{Z}[G])$ which supports an $n+1$-cubic structure then*

$$\mathcal{L}^{\otimes M_n} \simeq \mathcal{O}_H$$

where

$$M_n = M_n(G) = \prod_{k=2}^{n} \prod_{p, p | e(k)} \mathrm{ord}_p(\#G) \ .$$

Proof of Theorem 7.10. It follows from Theorem 7.8, Lemma 5.1, Lemma 5.2 and Remark 5.3 (in view of Remark 7.2 (b) and the fact that $\mathrm{Pic}(\mathbf{Z}) = (0)$). □

This combined with Remark 7.9 (a) gives

Corollary 7.11. *Let G be a finite abelian group and $1 \leq n \leq 4$. If $\mathcal{L}$ is an invertible sheaf on $H = G^D_{\mathrm{Spec}\,(\mathbf{Z})} = \mathrm{Spec}\,(\mathbf{Z}[G])$ which supports an $n+1$-cubic structure then $\mathcal{L} \simeq \mathcal{O}_H$.*

Proof of Proposition 7.5. Recall that we set $S = \mathrm{Spec}\,(\mathbf{Z})$. When $n = 1$ the Proposition follows from (6.13), Remark 7.4 and the fact that $\mathrm{H}^1(S, \mathbf{Z}/p^m) = (0)$. Now assume that $n \geq 2$ and let $r \geq 1$. Consider the homomorphisms

$$\delta_i : \mathrm{H}^1(\mu_r^{n-1}, \mathbf{Z}/r) \to \mathrm{H}^1(\mu_r^n, \mathbf{Z}/r), \quad 1 \leq i \leq n-1,$$

obtained as $m_i^* - p_i^* - q_i^*$ where

$$\begin{aligned}
m_i : \mu_r^n \to \mu_r^{n-1} \ ; \qquad (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, x_i x_{i+1}, \ldots, x_n),\\
p_i : \mu_r^n \to \mu_r^{n-1} \ ; \qquad (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, x_i, x_{i+2}, \ldots, x_n),\\
q_i : \mu_r^n \to \mu_r^{n-1} \ ; \qquad (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).
\end{aligned}$$

Lemma 7.12. *There is an exact sequence*

$$0 \to (n-1)\text{-}\mathrm{Ext}^1(\mu_r, \mathbf{Z}/r) \xrightarrow{t} \mathrm{H}^1(\mu_r^{n-1}, \mathbf{Z}/r) \xrightarrow{\oplus_i \delta_i} \bigoplus_{1 \leq i \leq n-1} \mathrm{H}^1(\mu_r^n, \mathbf{Z}/r).$$

where t is the forgetful map.

Proof. First suppose that P is a $\mathbf{Z}/r$-torsor over μ_r^{n-1} whose class $(P) \in \mathrm{H}^1(\mu_r^{n-1}, \mathbf{Z}/r)$ is in the kernel of all the homomorphisms δ_i, $1 \leq i \leq n-1$. We claim that there is a structure of $n-1$-extension on P: By our assumption, there are isomorphisms

$$c_i : p_i^* P \cdot q_i^* P \xrightarrow{\sim} m_i^* P \tag{7.3}$$

of $\mathbf{Z}/r$-torsors over μ_r^n. (We use $\cdot$ to denote the composition of $\mathbf{Z}/r$-torsors.) Let $e_k : S \to \mu_r^k$ be the identity section and set $P_0 = e_{n-1}^* P$; all $\mathbf{Z}/r$-torsors over $S = \mathrm{Spec}\,(\mathbf{Z})$ are trivial, so we can fix a trivialization $\alpha : \mathbf{Z}/r \xrightarrow{\sim} P_0$. There are natural isomorphisms $e_n^* m_i^* P \simeq P_0$, $e_n^* p_i^* P \simeq P_0$, $e_n^* q_i^* P \simeq P_0$. Hence we obtain an isomorphism of $\mathbf{Z}/r$-torsors over S

$$e_n^* c_i : P_0 \cdot P_0 \xrightarrow{\sim} P_0. \tag{7.4}$$

Using α we see that $e_n^* c_i$ becomes an isomorphism

$$\mathbf{Z}/r \cdot \mathbf{Z}/r \to \mathbf{Z}/r$$

which is necessarily given by addition in $\mathbf{Z}/r$ followed by translation by an element $a_i \in \mathrm{H}^0(S, \mathbf{Z}/r) = \mathbf{Z}/r$. Modify c_i by composing with the translation on $m_i^* P$ given by $-a_i$. We can now observe that the modified isomorphisms c_i satisfy the conditions of the partial composition laws (i.e of (4.4)) in the definition of $n-1$-extension: Indeed, this amounts to comparing certain isomorphisms of $\mathbf{Z}/r$-torsors over μ_r^k, $k = n$, $n+1$, $n+2$. Note that any two isomorphisms of $\mathbf{Z}/r$-torsors over μ_r^k differ by the addition of an element in $\mathrm{H}^0(\mu_n^k, \mathbf{Z}/r)$. Since μ_r^k is connected we have

$$\mathrm{H}^0(\mu_r^k, \mathbf{Z}/r) \xrightarrow[\sim]{e_k^*} \mathrm{H}^0(S, \mathbf{Z}/r) = \mathbf{Z}/r\ .$$

and so it is enough to compare the pull-backs of these isomorphisms via e_k. We can now see using the above discussion that these pull-backs agree.

It remains to show that the map $(n-1)\text{-}\mathrm{Ext}^1(\mu_r, \mathbf{Z}/r) \to \mathrm{H}^1(\mu_r^{n-1}, \mathbf{Z}/r)$ is injective: Suppose that a $\mathbf{Z}/r$-torsor P over μ_r^{n-1} with an $n-1$-extension structure given by the composition laws c_i as in (7.3) is trivial as a $\mathbf{Z}/r$-torsor. Pick a trivialization $\beta : (\mathbf{Z}/r)_{\mu_r^{n-1}} \xrightarrow{\sim} P$. This induces trivializations of $m_i^* P$, $p_i^* P$, $q_i^* P$ under which c_i is identified with

$$(\mathbf{Z}/r)_{\mu_r^n} \cdot (\mathbf{Z}/r)_{\mu_r^n} \to (\mathbf{Z}/r)_{\mu_r^n}$$

given by $(x, y) \mapsto x + y + a'_i$ with $a'_i \in \mathrm{H}^0(\mu_r^n, \mathbf{Z}/r) = \mathbf{Z}/r$. The compatibility condition (4.5) on the c_i's implies that a'_i is independent of the index i (see [SGA7I] VII 2.2 for a similar argument in the case of biextensions); we will denote it by a'. By composing β with the translation by $-a' \in \mathbf{Z}/r = \mathrm{H}^0(\mu_r^{n-1}, \mathbf{Z}/r)$ we can see that c_i becomes the map

$$(\mathbf{Z}/r)_{\mu_r^n} \cdot (\mathbf{Z}/r)_{\mu_r^n} \to (\mathbf{Z}/r)_{\mu_r^n}$$

given by addition. Therefore, P with the composition laws c_i is isomorphic to the trivial $n-1$-extension. $\square$

We now continue with the proof of Proposition 7.5. Lemma 7.12 applied to $r = p^m$ and (6.12) implies that, for $n \geq 2$, it is enough to show there is a natural isomorphism

$$\mathcal{C}(n; p^m) \xrightarrow{\sim} \ker(\mathrm{H}^1(\mu_{p^m}^{n-1}, \mathbf{Z}/p^m) \xrightarrow{\oplus_i \delta_i} \bigoplus_{1 \leq i \leq n-1} \mathrm{H}^1(\mu_{p^m}^n, \mathbf{Z}/p^m)).$$

To identify the kernel above, we will follow a technique used by Mazur in [M] §2. For the convenience of the reader we repeat some of Mazur's arguments. Suppose that X and Y are any two schemes equipped with $\mathbf{F}_p$-valued points

$$X \leftarrow \mathrm{Spec}\,(\mathbf{F}_p) \to Y. \tag{7.5}$$

We will use the symbol $X \vee Y$ to refer to any scheme theoretic union of X and Y along a subscheme which is a nilpotent extension of $\mathrm{Spec}\,(\mathbf{F}_p)$. For $Y = S = \mathrm{Spec}\,(\mathbf{Z})$ we set

$$\tilde{\mathrm{H}}^1(X, \mathbf{Z}/p^m) = \mathrm{H}^1(X \vee S, \mathbf{Z}/p^m)$$

(fppf or étale cohomology). There is an exact sequence

$$0 \to \tilde{\mathrm{H}}^1(X, \mathbf{Z}/p^m) \to \mathrm{H}^1(X, \mathbf{Z}/p^m) \to \mathrm{H}^1(\mathrm{Spec}\,(\mathbf{F}_p), \mathbf{Z}/p^m) \tag{7.6}$$

obtained using the Mayer-Vietoris exact sequence for étale cohomology, the fact that $\mathrm{Spec}\,(\mathbf{F}_p)$ is connected and that $\mathrm{H}^1(S, \mathbf{Z}/p^m) = (0)$. Hence, $\tilde{\mathrm{H}}^1(X, \mathbf{Z}/p^m)$ is independent of the exact scheme theoretic union of X and S used in the definition. A similar calculation, shows that for any diagram as in (7.5), we have

$$\tilde{\mathrm{H}}^1(X \vee Y, \mathbf{Z}/p^m) = \tilde{\mathrm{H}}^1(X, \mathbf{Z}/p^m) \oplus \tilde{\mathrm{H}}^1(Y, \mathbf{Z}/p^m). \tag{7.7}$$

Now set $T_{p^k} = \mathrm{Spec}\,(\mathbf{Z}[\zeta_{p^k}])$, $1 \le k \le m$; this is a closed subscheme of μ_{p^k}. Class-field theory gives a natural isomorphism

$$\mathrm{H}^1(T_{p^k}, \mathbf{Z}/p^m) \xrightarrow{\sim} \mathrm{Hom}(C(p^k), \mathbf{Z}/p^m).$$

Since the unique prime ideal of $\mathbf{Z}[\zeta_{p^k}]$ that lies above (p) is principal, by the exact sequence (7.6) and the definition of the Artin map, we have

$$\tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m) = \mathrm{H}^1(T_{p^k}, \mathbf{Z}/p^m) \xrightarrow{\sim} \mathrm{Hom}(C(p^k), \mathbf{Z}/p^m). \tag{7.8}$$

Now observe that we have canonical identifications

$$(\mathbf{Z}/p^k)^* = \mathrm{Aut}(\mu_{p^k}) = \mathrm{Aut}(T_{p^k})$$

where $a \in (\mathbf{Z}/p^k)^*$ acts via the operation "raising to the a-th power" on μ_{p^k}. The isomorphism (7.8) is compatible with the action of $(\mathbf{Z}/p^k)^*$ by functoriality of cohomology on the one side and by (7.2) on the other. If $\pi_k : T_{p^k} \to T_{p^{k-1}}$ is the natural projection, there is a commutative diagram

$$\begin{array}{ccccc} \tilde{\mathrm{H}}^1(T_{p^{k-1}}, \mathbf{Z}/p^m) & = & \mathrm{H}^1(T_{p^{k-1}}, \mathbf{Z}/p^m) & \xrightarrow{\sim} & \mathrm{Hom}(C(p^{k-1}), \mathbf{Z}/p^m) \\ \downarrow{\scriptstyle \pi_k^*} & & \downarrow{\scriptstyle \pi_k^*} & & \downarrow{\scriptstyle N_{k-1}} \\ \tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m) & = & \mathrm{H}^1(T_{p^k}, \mathbf{Z}/p^m) & \xrightarrow{\sim} & \mathrm{Hom}(C(p^k), \mathbf{Z}/p^m) \end{array} \tag{7.9}$$

with N_{k-1} induced by the norm. Now notice that $\mu^s_{p^m}$ for any $s \ge 1$, can be obtained as a wedge (in the sense of $\vee$ defined above) of several copies of T_{p^k}, $1 \le k \le m$, with S. More precisely, $\mu^s_{p^m}$ is the wedge of S with

$$\bigvee_{1 \le k \le m} \Big[\bigvee_{(a_1;\cdots;a_s) \in \mathbf{P}^{s-1}(\mathbf{Z}/p^k)} T_{p^k} \Big].$$

Using (7.7) we can deduce that

$$\mathrm{H}^1(\mu^s_{p^m}, \mathbf{Z}/p^m) = \bigoplus_{1 \le k \le m} \bigoplus_{(a_1;\cdots;a_s) \in \mathbf{P}^{s-1}(\mathbf{Z}/p^k)} \tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m). \tag{7.10}$$

Notice that an element $(a_i) = (a_1, \ldots, a_s) \in (p^{-k}\mathbf{Z}/\mathbf{Z})^s$ defines a group scheme homomorphism

$$(a_i) : \mu_{p^k} \to \mu^s_{p^m} \ ; \quad x \mapsto (x^{p^k a_1}, \ldots, x^{p^k a_t})$$

and a scheme morphism

$$(a_i) : T_{p^k} \subset \mu_{p^k} \to \mu^s_{p^m}.$$

Since $\pi_k(x) = x^p$ we have a commutative diagram

$$\begin{array}{ccc} T_{p^k} & \xrightarrow{(pa_i)} & \mu^s_{p^m} \\ {\scriptstyle \pi_k}\big\downarrow & & \big\| \\ T_{p^{k-1}} & \xrightarrow{(pa_i)} & \mu^s_{p^m}, \end{array} \tag{7.11}$$

where in the first, resp. second line, (pa_i) is considered as an element of $(p^{-k}\mathbf{Z}/\mathbf{Z})^s$, resp. of $(p^{-(k-1)}\mathbf{Z}/\mathbf{Z})^s$.

Set $U^s_{p^k} = (p^{-k}\mathbf{Z}/\mathbf{Z})^s - (p^{-k+1}\mathbf{Z}/\mathbf{Z})^s$; if (a_i) is in $U^s_{p^k}$ then the corresponding morphism is a closed immersion. Now consider the group of maps

$$\mathrm{Maps}_{(\mathbf{Z}/p^k)^*}(U^s_{p^k}, \tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m))$$

which are compatible with the natural action of $(\mathbf{Z}/p^k)^*$ on domain and range. Note that $\mathbf{P}^{s-1}(\mathbf{Z}/p^k) \simeq (\mathbf{Z}/p^k)^* \backslash U^s_{p^k}$. We can define a homomorphism

$$\mathrm{H}^1(\mu^s_{p^m}, \mathbf{Z}/p^m) \to \bigoplus_{1\leq k\leq m} \mathrm{Maps}_{(\mathbf{Z}/p^k)^*}(U^s_{p^k}, \tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m)) \tag{7.12}$$

by sending $h \in \mathrm{H}^1(\mu^s_{p^m}, \mathbf{Z}/p^m)$ to $(a_i) \mapsto (a_i)^* h$. Using (7.10) we see that (7.12) is an isomorphism. We can also consider the map

$$\mathrm{H}^1(\mu^s_{p^m}, \mathbf{Z}/p^m) \to \bigoplus_{1\leq k\leq m} \mathrm{Maps}_{(\mathbf{Z}/p^k)^*}((p^{-k}\mathbf{Z}/\mathbf{Z})^s, \tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m)) \tag{7.13}$$

given by the same rule as the one above. The map (7.13) is injective and using (7.11) we can see that its image is the subgroup of all elements $(\phi_k)_{1\leq k\leq m}$ which are such that $\phi_k((pa_i)) = \pi_k^* \phi_{k-1}((pa_i))$. Let us denote this subgroup by $F(s; p^m)$. By applying the above to $s = n-1$, n we can conclude that there are commutative diagrams

$$\begin{array}{ccc} \mathrm{H}^1(\mu^{n-1}_{p^m}, \mathbf{Z}/p^m) & \xrightarrow{\delta_i} & \mathrm{H}^1(\mu^n_{p^m}, \mathbf{Z}/p^m) \\ {\scriptstyle (7.13)_{n-1}}\big\downarrow & & \big\downarrow{\scriptstyle (7.13)_n} \\ F(n-1; p^m) & \xrightarrow{\delta'_i} & F(n; p^m) \end{array} \tag{7.14}$$

where the k-th component of $\delta'_i((\phi_k)_{1\leq k\leq m})$ is the map given by

$$(\ldots, a_i, a_{i+1}, \ldots) \mapsto \phi_k(\ldots, a_i + a_{i+1}, \ldots) - \phi_k(\ldots, a_i, \ldots) - \phi_k(\ldots, a_{i+1}, \ldots).$$

It now follows that the kernel of $\oplus_i \delta_i$ is isomorphic to the group of m-tuples $(\phi_k)_{1\leq k\leq m}$ of multilinear maps

$$\phi_k : (p^{-k}\mathbf{Z}/\mathbf{Z})^{n-1} \to \tilde{\mathrm{H}}^1(T_{p^k}, \mathbf{Z}/p^m) = \mathrm{Hom}(C(p^k), \mathbf{Z}/p^m)$$

which satisfy

$$\begin{array}{llcl} i) & \phi_k(ax_1, \ldots, ax_{n-1}) & = & \sigma_a(\phi_k(x_1, \ldots, x_{n-1})), \text{ for all } a \in (\mathbf{Z}/p^k)^*, \\ ii) & \phi_k(px_1, \ldots, px_{n-1}) & = & \pi_k^*(\phi_{k-1}(px_1, \ldots, px_{n-1})) \,. \end{array}$$

Note that a multilinear map $\phi_k : (p^{-k}\mathbf{Z}/\mathbf{Z})^{n-1} \to \mathrm{Hom}(C(p^k), \mathbf{Z}/p^m)$ has image which is contained in ${}_{p^k}\mathrm{Hom}(C(p^k), \mathbf{Z}/p^m) \simeq \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$; such a map is uniquely determined by $f_k := \phi_k(p^{-k}, \dots, p^{-k}) \in \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$. Using (7.9) and the multilinearity we see that conditions (i) and (ii) above translate to

$$\begin{array}{lrcl} i)' & \sigma_a(f_k) & = & a^{n-1} f_k, \text{ for all } a \in (\mathbf{Z}/p^k)^*, \\ ii)' & N_{k-1}(f_{k-1}) & = & p^{n-1} f_k\ . \end{array}$$

The proof of Proposition 7.5 now follows. □

Remark 7.13. We can see from the proof that the injective homomorphism

$$\psi_n : n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) \hookrightarrow \bigoplus_{1\le k\le m} \mathrm{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z}) \tag{7.15}$$

is obtained as follows: Consider the homomorphism

$$\psi'_n : n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) \to \mathrm{H}^1(\mu_{p^m}, \mathbf{Z}/p^m), \tag{7.16}$$

defined as the composition

$$\begin{aligned} n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) \to (n-1)\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{Z}/p^m) \xrightarrow{t} \\ \xrightarrow{t} \mathrm{H}^1(\mu_{p^m}^{n-1}, \mathbf{Z}/p^m) \xrightarrow{\Delta^*_{n-1}} \mathrm{H}^1(\mu_{p^m}, \mathbf{Z}/p^m) \end{aligned}$$

where the first arrow is the inverse of (6.12), t is the forgetful map and Δ^*_{n-1} is the pull-back along the diagonal $\Delta_{n-1} : \mu_{p^m} \to \mu_{p^m}^{n-1}$. Then ψ_n is given by the composition of ψ'_n with the isomorphism

$$\mathrm{H}^1(\mu_{p^m}, \mathbf{Z}/p^m) \xrightarrow{\sim} \bigoplus_{1\le k\le m} \mathrm{Hom}(C(p^k), p^{-m}\mathbf{Z}/\mathbf{Z})$$

obtained by (7.8) and (7.10). Indeed, the maps ϕ_k in the proof of the Proposition are determined by their image on the "diagonal" elements $(p^{-k}, \dots, p^{-k})$.

8. Reflection homomorphisms

In the next few paragraphs, we elaborate on the constructions of the previous section. We continue with the same assumptions and notations. In particular, we again write $T_{p^k} = \mathrm{Spec}\,(\mathbf{Z}[\zeta_{p^k}])$ which we think of as a closed subscheme of μ_{p^k}. We will denote by $\widetilde{\mu_{p^m}} = \bigsqcup_{0\le k\le m} T_{p^k}$ the normalization of the scheme μ_{p^m} and by $\nu : \widetilde{\mu_{p^m}} \to \mu_{p^m}$ the natural projection map. Our main goal is to express the composition

$$n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) \xrightarrow{t} \mathrm{Pic}(\mu_{p^m}^n) \xrightarrow{\Delta^*_n} \mathrm{Pic}(\mu_{p^m}) \xrightarrow{\nu^*} \mathrm{Pic}(\widetilde{\mu_{p^m}}) \tag{8.1}$$

in terms of the classical "reflection homomorphisms" (see below). We do this in Corollary 8.2. We can then deduce some additional results on the pull-back $\nu^*\mathcal{L}$ of an invertible sheaf $\mathcal{L}$ on μ_{p^m} with hypercubic structure.

8.a. Consider the homomorphism (6.16) described in 6.d

$$R_k : \mathrm{H}^1(T_{p^k}, \mathbf{Z}/p^k) \to {}_{p^k}\mathrm{Pic}(T_{p^k}) \ ; \quad Q \mapsto \mathcal{L}^Q_{f(\chi_0)}$$

for $G = \mathbf{Z}/p^k$, $S' = T' = T = T_{p^k}$, $\chi_0 : T \hookrightarrow \mu_{p^k}$ the natural closed immersion which corresponds to the character $\chi_0 : \mathbf{Z}/p^k \to \mathbf{Z}[\zeta_{p^k}]^*$, $\chi_0(1) = \zeta_{p^k}$, and $f(\chi_0) : T' = T \to \mu_{p^k}{}_T$ the morphism

$$f(\chi_0) : T \xrightarrow{\Delta} T \times_S T \xrightarrow{(\chi_0, \mathrm{id})} \mu_{p^k}{}_T = \mu_{p^k} \times T.$$

Using (7.8) (class field theory) and $C(p^k) = \mathrm{Pic}(T_{p^k})$ we see that this amounts to a homomorphism

$$R_k : \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \to {}_{p^k}C(p^k).$$

If $Q \to T_{p^k}$ is a $\mathbf{Z}/p^k$-torsor there is an unramified Galois extension N of $\mathbf{Q}(\zeta_{p^k})$ with Galois group $\mathbf{Z}/p^k$ and ring of integers $\mathcal{O}_N$ such that the $\mathbf{Z}/p^k$-torsor Q is $Q = \mathrm{Spec}\,(\mathcal{O}_N)$. Lemma 6.1 implies that $\mathcal{L}^Q_{f(\chi_0)}$ is isomorphic to the invertible sheaf which corresponds to the locally free rank 1 $\mathbf{Z}[\zeta_{p^k}]$-module

$$L^Q_{\chi_0} := \{\xi \in \mathcal{O}_N \mid \sigma_a(\xi) = \chi_0^{-1}(a)\xi = \zeta_{p^k}^{-a}\xi, \text{ for all } a \in \mathbf{Z}/p^k\}. \tag{8.2}$$

Notice that $N/\mathbf{Q}(\zeta_{p^k})$ is a Kummer extension. Therefore, it can be obtained by adjoining the p^k-th root of an element $b \in \mathbf{Q}(\zeta_{p^k})^*$: $N = \mathbf{Q}(\zeta_{p^k})(\sqrt[p^k]{b})$. We can arrange so that the element $\sqrt[p^k]{b}$ gives a generic section of $\mathcal{L}^Q_{f(\chi_0)}$; the corresponding divisor of $\mathcal{L}^Q_{f(\chi_0)}$ is given by a fractional ideal I of $\mathbf{Q}(\zeta_{p^k})$ such that $I^{p^k} = (b)$. The class of $\mathcal{L}^Q_{f(\chi_0)}$ corresponds to the class (I) under the isomorphism $\mathrm{Pic}(T_{p^k}) \simeq C(p^k)$. Using this we can see that R_k coincides with the classical *"reflection homomorphism"*

$$\mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \to {}_{p^k}C(p^k)$$

(see for example [W] §10.2 for the case $k = 1$; actually the reflection homomorphism defined there is the negative of the one above):

Now observe that the definition of $\mathcal{L}^Q_{f(\chi_0)}$ implies

$$a^*(\mathcal{L}^Q_{f(\chi_0)}) \simeq \mathcal{L}^{a^*Q}_{f(\chi_0^a)}, \quad a \in (\mathbf{Z}/p^k)^*,$$

where a^* denotes the pull-back by the Galois automorphism $a : T_{p^k} \to T_{p^k}$. Using (6.18) we see that this gives

$$a^*(\mathcal{L}^Q_{f(\chi_0)}) \simeq \mathcal{L}^{a^*Q}_{f(\chi_0^a)} \simeq (\mathcal{L}^{a^*Q}_{f(\chi_0)})^{\otimes a}. \tag{8.3}$$

The isomorphism (8.3) now implies that R_k "reflects" between odd and even eigenspaces, in fact it decomposes into a direct sum of

$$\begin{aligned} R_k^{(n)} : \mathrm{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z}) = \\ = \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})^{(n-1)} \to ({}_{p^k}C(p^k))^{(n)}. \end{aligned} \tag{8.4}$$

for $0 \leq n \leq p-2$ (cf. [W] §10.2).

8.b. For notational simplicity, we set $r = p^m$. Recall $\nu : \widetilde{\mu_r} \to \mu_r$ is the normalization morphism. Let us consider the homomorphism

$$\mathrm{H}^1(\mu_r, \mathbf{Z}/r) \to \mathrm{Pic}(\mu_r) \xrightarrow{\nu^*} \mathrm{Pic}(\widetilde{\mu_r}) = \bigoplus_{1\le k\le m} C(p^k) \tag{8.5}$$

where the first arrow is the composition

$$\mathrm{H}^1(\mu_r, \mathbf{Z}/r) \xrightarrow{(6.13)} \mathrm{Ext}^1(\mu_{r\,\mu_r}, \mathbf{G}_{m\,\mu_r}) \xrightarrow{t} \mathrm{Pic}(\mu_r \times \mu_r) \xrightarrow{\Delta_2^*} \mathrm{Pic}(\mu_r). \tag{8.6}$$

Recall that (7.8) and (7.10) give an isomorphism

$$\mathrm{H}^1(\mu_r, \mathbf{Z}/r) \xrightarrow{\sim} \bigoplus_{1\le k\le m} \mathrm{Hom}(C(p^k), p^{-m}\mathbf{Z}/\mathbf{Z}). \tag{8.7}$$

Now let us restrict the map (8.5) to the subgroup of $\mathrm{H}^1(\mu_r, \mathbf{Z}/r)$ that corresponds to

$$\bigoplus_{1\le k\le m} \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z})$$

under (8.7). We obtain a homomorphism

$$R : \bigoplus_{1\le k\le m} \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \to \bigoplus_{1\le k\le m} C(p^k). \tag{8.8}$$

By unraveling the definition of R we see that the description of "reflection homomorphisms" in the above paragraph implies that

Proposition 8.1. *The homomorphism R is a direct sum $R = \oplus_{1\le k\le m} R_k$ with*

$$R_k : \mathrm{Hom}(C(p^k), p^{-k}\mathbf{Z}/\mathbf{Z}) \to {}_{p^k}C(p^k)$$

the "reflection homomorphism" as defined above. □

We now obtain:

Corollary 8.2. *There is a commutative diagram*

$$\begin{array}{ccccccc}
n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) & \xrightarrow{t} & \mathrm{Pic}(\mu_{p^m}^n) & \xrightarrow{\Delta_n^*} & \mathrm{Pic}(\mu_{p^m}) & \xrightarrow{\nu^*} & \mathrm{Pic}(\widetilde{\mu_{p^m}}) \\
\psi_n\downarrow & & & & & & \cup \\
\bigoplus_{1\le k\le m} \mathrm{Hom}((C(p^k)/p^k)^{(1-n)}, p^{-k}\mathbf{Z}/\mathbf{Z}) & & \xrightarrow{\oplus_{1\le k\le m} R_k^{(n)}} & & & & \bigoplus_{1\le k\le m} ({}_{p^k}C(p^k))^{(n)}.
\end{array}$$

Proof. Recall that by Remark 7.13, the homomorphism ψ_n is given by the composition of $\psi_n' : n\text{-}\mathrm{Ext}^1(\mu_{p^m}, \mathbf{G}_m) \to \mathrm{H}^1(\mu_{p^m}, \mathbf{Z}/p^m)$ with the isomorphism (8.7). The result follows now from the definitions of the homomorphisms R and ψ_n', Proposition 8.1, and the commutative diagram (6.15) for $H = \mu_{p^m}$: Indeed, we can observe that the composite homomorphism (8.6) essentially gives a half of the commutative diagram (6.15) for $H = \mu_{p^m}$. □

Remark 8.3. If the prime p satisfies the Kummer-Vandiver conjecture, then the reflection maps $R_k^{(n)}$ are all trivial; indeed, either n or $1-n$ is even and so either $({}_{p^k}C(p^k))^{(n)}$ or $(C(p^k)/p^k)^{(1-n)}$ is trivial ([W] Cor. 10.6). Then the composition $\nu^* \cdot \Delta_n^* \cdot t$ along the first row of the above diagram is also the trivial homomorphism.

8.c. We now combine the above to obtain an additional result about invertible sheaves with hypercubic structures over $H = \mathrm{Spec}\,(\mathbf{Z}[G])$, for G any finite abelian group. For an integer $u \geq 1$ set

$$e'(u) = \begin{cases} 1 & , \text{ if } u \text{ is odd,} \\ \text{numerator}\,(B_u/u) & , \text{ if } u \text{ is even.} \end{cases}$$

(cf. Remark 7.9 (b)). Set

$$M_n'(G) = \prod_{u=1}^{n} \prod_{p|e'(u)} \mathrm{ord}_p(\#G).$$

Theorem 8.4. *Assume that all the prime divisors of $\#G$ satisfy the Kummer-Vandiver conjecture. We denote by $\nu : \widetilde{H} \to H$ the normalization morphism. Suppose that $\mathcal{L}$ is an invertible sheaf on H which supports an $n+1$-cubic structure ξ and set $C = \mathrm{GCD}(M_n'(G), n!!)$. Then $\nu^*\mathcal{L}^{\otimes C} \simeq \mathcal{O}_{\widetilde{H}}$. In particular, if in addition all the prime divisors of $\#G$ are $\geq n+1$, then $\nu^*\mathcal{L} \simeq \mathcal{O}_{\widetilde{H}}$.*

Proof. Suppose that $G = G_{p_1} \times \cdots \times G_{p_k}$ is the decomposition of G into its p-Sylow subgroups. Set $H_{p_j} = (G_{p_j})^D = \mathrm{Spec}\,(\mathbf{Z}[G_{p_j}])$ and let $\mathrm{pr}_j : H \to H_{p_j}$ be the natural projection. If all the prime divisors p_j, $1 \leq j \leq k$, of $\#G$ satisfy the Kummer-Vandiver conjecture we have $\mathcal{L}^{\otimes M_n'(G)} \simeq \mathcal{O}_H$ by Theorem 7.10 (cf. Remark 7.9 (b)). On the other hand, Corollary 5.6 gives the "Taylor expansion"

$$\nu^*\mathcal{L}^{\otimes n!!} \simeq \bigotimes_{i=0}^{n-1} (\nu^*\Delta_{n-i}^* E(\mathcal{L}^{(i)}, \xi^{(i)}))^{\otimes(-1)^i(n-i-1)!!} \otimes \nu^* 0^* \mathcal{L}^{\otimes n!!}.$$

Here, the invertible sheaf $E(\mathcal{L}^{(i)}, \xi^{(i)})$ carries the structure of an $(n-i)$-extension of H by $\mathbf{G}_m$. Notice that, since $\mathrm{Pic}(\mathbf{Z}) = (0)$, $0^*\mathcal{L}$ is trivial. Our goal is to show that the invertible sheaves $\nu^*\Delta_{n-i}^* E(\mathcal{L}^{(i)}, \xi^{(i)})$, $0 \leq i \leq n-1$, are also trivial. This would imply that we have $\nu^*\mathcal{L}^{\otimes n!!} \simeq \mathcal{O}_{\widetilde{H}}$ from which, given the above discussion, the result follows. Observe that (6.8) implies that there is an isomorphism of multiextensions

$$E(\mathcal{L}^{(i)}, \xi^{(i)}) \simeq \bigotimes_{j=1}^{k} (\mathrm{pr}_j \times \cdots \times \mathrm{pr}_j)^*(E_j^i)\ , \tag{8.9}$$

where E_j^i is an $(n-i)$-extension of H_{p_j} by $\mathbf{G}_m$. Using (8.9) we see that it is enough to prove that the invertible sheaves $\nu^*\Delta_{n-i}^*(E_j^i)$ are trivial, where now ν and Δ_{n-i} are the normalization and diagonal morphisms for the group scheme H_{p_j}. In fact, since the normalization $\widetilde{H}_{p_j}$ is the disjoint union of components corresponding to characters of G_{p_j} and these factor through prime power order cyclic quotients we can see that we can reduce to the case of a prime power order cyclic group. More precisely, it is enough to show the

following statement: If E is an $(n-i)$-extension of μ_{p^m} by $\mathbf{G}_m$, then the invertible sheaf $\nu^*\Delta^*_{n-i}(E)$ is trivial. Corollary 8.2 applied to $n-i$ implies that the composition

$$(n-i)\text{-Ext}^1(\mu_{p^m}, \mathbf{G}_m) \xrightarrow{t} \mathrm{Pic}(\mu_{p^m}^{n-i}) \xrightarrow{\nu^*\Delta^*_{n-i}} \mathrm{Pic}(\widetilde{\mu_{p^m}}) \tag{8.10}$$

factors through the reflection homomorphisms. Hence, if p satisfies the Kummer-Vandiver conjecture then the homomorphism (8.10) is trivial (Remark 8.3). Therefore, the invertible sheaves $\nu^*\Delta^*_{n-i}(E)$ are trivial. The result now follows. □

8.d. Suppose that $G = \mathbf{Z}/p$ and that $\mathcal{L}$ is an invertible sheaf on μ_p which supports an $d+2$-cubic structure ξ with $p > d+1$. As above, Corollary 5.6 gives

$$\nu^*\mathcal{L}^{\otimes(d+1)!!} \simeq \bigotimes_{i=0}^{d} \nu^*(\Delta^*_{d+1-i}E(\mathcal{L}^{(i)}, \xi^{(i)}))^{\otimes(-1)^i(d-i)!!}.$$

Since, by Theorem 7.10, the invertible sheaf $\mathcal{L}$ is p-power torsion and $\mathrm{GCD}(p, (d+1)!!) = 1$, we can write

$$\nu^*\mathcal{L} \simeq \bigotimes_{i=0}^{d} \nu^*\Delta^*_{d+1-i}E'_{d+1-i},$$

where E'_{d+1-i} is an invertible sheaf on μ_p^{d+1-i} with a $(d+1-i)$-extension structure. Let us denote by $t_j(\mathcal{L}, \xi)$ the image of E'_j under the homomorphism

$$\psi_j : j\text{-Ext}^1(\mu_p, \mathbf{G}_m) \to \mathrm{Hom}((C(p)/p)^{(1-j)}, p^{-1}\mathbf{Z}/\mathbf{Z})$$

of Proposition 7.5 (In this case, ψ_j is an isomorphism; cf. Corollary 7.7). By [Ri], the pull back $\nu^* : \mathrm{Pic}(\mu_p) \to \mathrm{Pic}(\tilde{\mu}_p) = \mathrm{Cl}(\mathbf{Q}(\zeta_p))$ is an isomorphism and we can use it to identify these class groups. Therefore, Corollary 8.2 and the above equality now implies that we can write

$$[\mathcal{L}] = \sum_{j=1}^{d+1} R^{(j)}(t_j(\mathcal{L}, \xi)) \tag{8.11}$$

in $\mathrm{Pic}(\mu_p) = \mathrm{Cl}(\mathbf{Q}(\zeta_p))$ with $R^{(j)} = R_1^{(j)} : \mathrm{Hom}((C(p)/p)^{(1-j)}, p^{-1}\mathbf{Z}/\mathbf{Z}) \to ({}_pC(p))^{(j)}$ the reflection homomorphism.

9. The hypercubic structure on the determinant of cohomology

In this section, we explain some of the results of F. Ducrot [Du] and we show how the work in [Du] can be used to deduce the main result in this section, Theorem 9.8.

For every non-empty finite set I we denote by $C(I)$ the set of all subsets of I. Suppose that $\mathcal{P}$ is a s.c. Picard category (§2.a). By definition, an *I-cube* in $\mathcal{P}$ is a family $K = (K_v)_{v \in C(I)}$ of objects of $\mathcal{P}$, indexed by the set $C(I)$ of all subsets of I. We denote by *I-$Cube(\mathcal{P})$* the category of I-cubes in $\mathcal{P}$.

If $n \geq 1$, then an *n-cube* in $\mathcal{P}$ is by definition an I-cube in $\mathcal{P}$ for some I with $\#I = n$. A morphism between two n-cubes $K = (K_v)_{v \in C(I)}$, $K' = (K'_w)_{w \in C(I')}$ is a pair $\Phi = (\varphi, \phi)$

where $\varphi : I \xrightarrow{\sim} I'$ is bijective and $\phi : K \xrightarrow{\sim} \varphi^*(K')$ is an (iso)morphism of I-cubes. The category of all n-cubes in $\mathcal{P}$ will be denoted by n-$Cube(\mathcal{P})$.

This "cubic" terminology is motivated by the fact that if $I = \{1, 2, \ldots, n\}$ we may think of $C(I)$ as the vertices of the standard n-dimensional cube C_n in $\mathbf{R}^n$ by sending a subset $v \subset I$ to the point $(v_i)_{1\leq i\leq n}$ with $v_i = 1$ if $i \in v$, $v_i = 0$ if $i \notin v$. Hence, after choosing an order for I, we can visualize the objects K_v of an I-cube K as being placed on the vertices of the n-dimensional cube C_n.

For $v \in C(I)$, set $s(v) = (-1)^{\#I-\#v}$. If K is an n-cube in $\mathcal{P}$ we now set

$$\Sigma(K) = \sum_{v\in C(I)} (-1)^{s(v)} K_v \tag{9.1}$$

(cf. Lemma 2.1). We can see that an isomorphism $\Phi : K \to K'$ between n-cubes induces an isomorphism

$$\Sigma(\Phi) : \Sigma(K) \xrightarrow{\sim} \Sigma(K') \tag{9.2}$$

in $\mathcal{P}$. In fact, we obtain a functor $\Sigma : n\text{-}Cube(\mathcal{P}) \to \mathcal{P}$.

Suppose that K is an I-cube and let J_0, J be disjoint subsets of I with $\#J = q$. We call the J-cube $(K_{J_0\cup J'})_{J'\subset J}$ a q-face of K. If $i \in I$, we will denote by $\mathrm{Front}_i(K)$, $\mathrm{Back}_i(K)$ the $I - \{i\}$-cubes given by $J_0 = \{i\}$, $J_0 = \emptyset$. We may think of $\mathrm{Front}_i(K)$, $\mathrm{Back}_i(K)$ as the two "opposite" $n-1$-faces of K obtained by restricting the i-th coordinate to be equal to 1, resp. 0. There is a canonical isomorphism (cf. Lemma 2.1)

$$\Sigma(\mathrm{Front}_i(K)) + (-\Sigma(\mathrm{Back}_i(K))) \xrightarrow{\sim} \Sigma(K). \tag{9.3}$$

Conversely, if $I = J \cup \{i\}$ and A, B are two J-cubes, we will denote by $A \overset{i}{—} B$ the I-cube whose i-th back face and i-th front face are respectively A and B. We obtain a canonical isomorphism

$$\Sigma(B) + (-\Sigma(A)) \xrightarrow{\sim} \Sigma(A \overset{i}{—} B). \tag{9.4}$$

Definition 9.1. By definition, a *decorated n-cube* in $\mathcal{P}$ is an n-cube K together with isomorphisms ("2-face trivializations")

$$m_F : \underline{O} \xrightarrow{\sim} \Sigma(F), \tag{9.5}$$

for each 2-face F of K, which satisfy the following condition: Suppose that L is a 3-face of K which corresponds to the subsets J_0 and J as above. For each pair of indices $i, j \in J$ the 2-face trivializations for $\mathrm{Front}_i(L)$, $\mathrm{Back}_i(L)$, $\mathrm{Front}_j(L)$, $\mathrm{Back}_j(L)$ should be compatible with the canonical isomorphism given by (9.3)

$$\Sigma(\mathrm{Front}_i(L)) + (-\Sigma(\mathrm{Back}_i(L))) \xrightarrow{\sim} \Sigma(L) \xrightarrow{\sim} \Sigma(\mathrm{Front}_j(L)) + (-\Sigma(\mathrm{Back}_j(L))). \tag{9.6}$$

9.a. Now let $\mathfrak{S}$ be a site and suppose that $a : \mathcal{P} \to \mathfrak{S}$ is a s.c. Picard $\mathfrak{S}$-stack. For our applications, $\mathfrak{S} = S_{\rm fppf}$. A (decorated) n-cube K in $\mathcal{P}$ is a (decorated) n-cube in the fiber category $\mathcal{P}_T$ for some $T \in {\rm Ob}(\mathfrak{S})$; in particular, all the objects K_v, $v \in C(I)$, satisfy $a(K_v) = T$.

The n-cubes in $\mathcal{P}$ form naturally an $\mathfrak{S}$-stack n-$Cube(\mathcal{P})$. There is also an $\mathfrak{S}$-stack n-$Cube_d(\mathcal{P})$ whose objects are decorated n-cubes in $\mathcal{P}$, and morphisms are given by morphisms $\Phi = (\varphi, \phi) : K \to K'$ in n-$Cube(\mathcal{P})$ which are compatible with the isomorphisms (9.5) in the following sense: If $F' \subset K'$ is a 2-face, then let F be the corresponding (via φ) 2-face of K. Let $a(\Phi) = \tau : T \to T'$. We ask that the following diagram commutes:

$$\begin{array}{ccc} \underline{O}_T & \xrightarrow{m_F} & \Sigma(F) \\ \Big\downarrow & & \Big\downarrow \Sigma(\Phi_{|F}) \\ \underline{O}_{T'} & \xrightarrow{m_{F'}} & \Sigma(F') \ ; \end{array} \tag{9.7}$$

here the left vertical arrow is the canonical morphism lifting $\tau : T \to T'$ and we denote by $\Phi_{|F} : F \to F'$ the isomorphism of 2-cubes obtained from Φ "by restriction".

Now suppose that K, K' are two I-cubes in $\mathcal{P}$ and let $u : {\rm Front}_i(K) \xrightarrow{\sim} {\rm Back}_i(K')$ be an isomorphism of $I - \{i\}$-cubes for some $i \in I$. Then we can define the "glueing" $K *_i K'$ of K and K' along u; this is an I-cube with ${\rm Back}_i(K *_i K') = {\rm Back}_i(K)$, ${\rm Front}_i(K *_i K') = {\rm Front}_i(K')$. By combining the isomorphisms given by (9.3) with $\Sigma(u)$ we obtain a natural isomorphism

$$\Sigma(K *_i K') \xrightarrow{\sim} \Sigma(K) + \Sigma(K'). \tag{9.8}$$

If both K and K' are decorated and the isomorphism u is compatible with the 2-face trivializations in the sense above (i.e if it is an isomorphism of decorated cubes), then $K *_i K'$ becomes naturally a decorated I-cube with 2-face trivializations induced by those of K and K' ([Du] §1.5). Also note that for $i \in I$, $J = I - \{i\}$, if A is a decorated J-cube, then the I-cube $A \overset{i}{—} A$ is also naturally decorated.

9.b. Let $\mathcal{P}$, $\mathcal{Q}$ be two s.c. Picard $\mathfrak{S}$-stacks and suppose that $\delta : \mathcal{P} \to \mathcal{Q}$ is an $\mathfrak{S}$-functor. We will also denote by δ the $\mathfrak{S}$-functor

$$\delta : n\text{-}Cube(\mathcal{P}) \to n\text{-}Cube(\mathcal{Q})$$

which sends the I-cube $K = (K_v)_{v \in C(I)}$ to $(\delta(K_v))_{v \in C(I)}$.

Compose with $\Sigma : n$-$Cube(\mathcal{Q}) \to \mathcal{Q}$ to obtain a functor:

$$\delta^n := \Sigma \cdot \delta : n\text{-}Cube(\mathcal{P}) \to \mathcal{Q} \ ; \quad \delta^n(K) = \sum_{v \in C(I)} (-1)^{s(v)} \delta(K_v) \ .$$

We can observe that if K, K' are I-cubes with an isomorphism $u : {\rm Front}_i(K) \xrightarrow{\sim} {\rm Back}_i(K')$, $i \in I$, then by using (9.8) we can obtain a (natural) isomorphism

$$\delta^n(K *_i K') \xrightarrow{\sim} \delta^n(K) + \delta^n(K'). \tag{9.9}$$

Also notice that for $i \in I$, $J = I - \{i\}$, and A a decorated J-cube, (9.4) provides us with an isomorphism

$$\underline{O} \xrightarrow{\sim} \delta^n(A \overset{i}{—} A). \tag{9.10}$$

We can now restrict δ^n to decorated n-cubes to obtain a functor

$$\delta^n : n\text{-}Cube_d(\mathcal{P}) \to \mathcal{Q}\,.$$

Let us also consider the trivial functor

$$e : n\text{-}Cube_d(\mathcal{P}) \to \mathcal{Q}\ ; \quad e(K) = \underline{O},\ e(\Phi) = \mathrm{Id}_{\underline{O}}.$$

Definition 9.2. (Ducrot [Du]) An n-cubic structure on δ is an $\mathfrak{S}$-functor isomorphism

$$\Xi : e \xrightarrow{\sim} \delta^n$$

(between functors on decorated n-cubes) which satisfies the following "glueing" condition: If K, K' are decorated I-cubes, $\#I = n$, with a (compatible) isomorphism $u : \mathrm{Front}_i(K) \xrightarrow{\sim} \mathrm{Back}_i(K')$, for some $i \in I$, then the diagram

$$\begin{array}{ccc}
\underline{O} + \underline{O} & \xrightarrow{\Xi(K)+\Xi(K')} & \delta^n(K) + \delta^n(K') \\
\wr\big\uparrow & & \big\uparrow{\scriptstyle (9.9)} \\
\underline{O} & \xrightarrow{\Xi(K *_i K')} & \delta^n(K *_i K')
\end{array}$$

is commutative.

Remark 9.3. a) In [Du], one actually finds a definition of the notion of n-cubic structure on a functor $\delta : \mathcal{P} \to \mathcal{Q}$ where $\mathcal{Q}$ is a Picard stack which is not necessarily strictly commutative. This definition involves a functor $\Sigma : n\text{-}Cube(\mathcal{Q}) \to \mathcal{Q}$ ([Du] 1.3.2) which generalizes the functor Σ given in the strictly commutative case above. (Roughly speaking, to define Σ, Ducrot adjusts our "naive" definition by using an appropriate combination of the signs $\varepsilon(K_v)$ that give the obstruction to strict commutativity; when $\mathcal{Q}$ is s.c. this coincides with the definition that we have used here). This definition of n-cubic structure in [Du] also includes an additional condition:

("Normalization") For $i \in I$, A a decorated $I - \{i\}$-cube and $K = (A \overset{i}{—} A)$ the corresponding decorated I-cube, the isomorphism $\Xi(K) : \underline{O} \xrightarrow{\sim} \delta^n(K)$ is equal to the isomorphism (9.10).

We can see that when $\mathcal{Q}$ is s.c this normalization condition is implied by the glueing condition above. Hence, in this case, the definition above is equivalent to the definition of [Du]. Indeed, apply the glueing condition to $K = K' = (A \overset{i}{—} A)$ with u the identity. We have $K *_i K = K$ and so we obtain a commutative diagram

$$\begin{array}{ccc}
\underline{O} + \underline{O} & \xrightarrow{\Xi(K)+\Xi(K)} & \delta^n(K) + \delta^n(K) \\
\wr\big\uparrow & & \big\uparrow{\scriptstyle (9.9)} \\
\underline{O} & \xrightarrow{\Xi(K)} & \delta^n(K).
\end{array}$$

Now observe that in the s.c. Picard stack $\mathcal{Q}$, there is a similar commutative diagram but with $\Xi(K)$ replaced by the isomorphism (9.10). This implies that $\Xi(K)$ coincides with (9.10) since the pair $(\underline{O}, \epsilon)$ of an identity object of $\mathcal{Q}$ together with $\epsilon : \underline{O}+\underline{O} \xrightarrow{\sim} \underline{O}$ is unique up to *unique* isomorphism.

b) Suppose that K is a decorated I-cube for $I = \{1, \dots, n\}$ and let $\sigma \in S_n$. The permutation σ induces a morphism of decorated n-cubes $\sigma : \sigma^* K \to K$. This provides us with an isomorphism

$$\delta^n(\sigma) : \delta^n(\sigma^* K) \xrightarrow{\sim} \delta^n(K). \tag{9.11}$$

Since Ξ is supposed to be a functor isomorphism we must have

$$\delta^n(\sigma) \cdot \Xi(\sigma^* K) = \Xi(K). \tag{9.12}$$

9.c. It follows directly from the definitions that an additive $\mathfrak{S}$-functor $F : \mathcal{P} \to \mathcal{Q}$ induces an $\mathfrak{S}$-functor between decorated n-cubes

$$F : n\text{-}Cube_d(\mathcal{P}) \to n\text{-}Cube_d(\mathcal{Q}) \ . \tag{9.13}$$

Lemma 9.4. *If $\delta : \mathcal{P} \to \mathcal{Q}$ supports an n-cubic structure and $F : \mathcal{P}' \to \mathcal{P}$ is an additive functor, then the composite $\delta \cdot F : \mathcal{P}' \to \mathcal{Q}$ also supports an n-cubic structure.*

Proof. Since by definition $(\delta \cdot F)^n = \delta^n \cdot F$, a trivialization Ξ of δ^n defines a trivialization of $(\delta \cdot F)^n$. Now if K, K' are decorated I-cubes with a (compatible) isomorphism u : $\mathrm{Front}_i(K) \xrightarrow{\sim} \mathrm{Back}_i(K')$, then $F(u)$ gives a compatible isomorphism between the i-th front and i-th back faces of $F(K)$ and $F(K')$ respectively and we have

$$F(K) *_i F(K') = F(K *_i K') \tag{9.14}$$

(as decorated I-cubes). We can now see using (9.14) that the above trivialization satisfies the glueing property of the definition. □

9.d. Recall that we denote by $\mathcal{PIC}(T)$ the s.c. Picard $S_{\rm fppf}$-stack given by invertible $\mathcal{O}_{T\times_S S'}$-sheaves on the schemes $T \times_S S'$, $S' \to S$ a fppf morphism. Let $H \to S$ be a fppf abelian group scheme. By Yoneda equivalence, there is natural bijection between $S_{\rm fppf}$-functors $\delta : H \to \mathcal{PIC}(S)$ (where H also denotes the s.c. Picard stack represented by the group scheme) and invertible $\mathcal{O}_H$-sheaves on the scheme H given by $\delta \mapsto \mathcal{L}_\delta := \delta(H \xrightarrow{\rm id} H)$.

Lemma 9.5. *Suppose that the functor $\delta : H \to \mathcal{PIC}(S)$ supports an n-cubic structure in the sense of Definition 9.2 above. Then the invertible sheaf $\mathcal{L}_\delta$ over H is equipped with an n-cubic structure in the sense of Definition 3.1.*

Proof. For simplicity, set $\mathcal{L} = \mathcal{L}_\delta$. Let $I = \{1, \dots, n\}$. We can see that, since the Picard stack H is discrete, decorated I-cubes in H correspond bijectively to ordered $n+1$-tuples $(a_i)_i$, $i = 0, \dots, n$, of S'-valued points $a_i \in H(S')$:

$$(a_i)_i \mapsto K_{a_0}(a_1, \dots, a_n) := \text{the cube given by } K_v = a_0 + \sum_{i, v_i = 1} a_i. \tag{9.15}$$

For simplicity, if $a_0 = 0$, we will denote the above cube by $K(a_1, \ldots, a_n)$. Now notice that, by the definition of δ^n, there is a canonical isomorphism

$$\delta^n(K(a_1, \ldots, a_n)) \simeq (a_1, \ldots, a_n)^* \Theta_n(\mathcal{L}). \tag{9.16}$$

First suppose that δ supports an n-cubic structure Ξ; then by (9.16), the functor isomorphism Ξ evaluated at the n-cube $K(a_1, \ldots, a_n)$ with $S' = H^n$ and $a_i = \mathrm{pr}_i : H^n \to H$, gives a trivialization ξ of the invertible sheaf $\Theta_n(\mathcal{L})$ over H^n. Now take all $a_i = 0$ (as S-points) and set for simplicity $K(\underline{0}) = K(0, \ldots, 0)$. The n-cubic structure Ξ provides us with an isomorphism

$$\Xi(K(\underline{0})) : \mathcal{O}_S \xrightarrow{\sim} \delta^n(K(\underline{0}))$$

which by Remark 9.3 (a) agrees with the natural $\mathcal{O}_S \xrightarrow{\sim} \delta^n(K(\underline{0}))$ given by the contraction isomorphisms. In view of (9.16) this implies that ξ satisfies Property (c0) of Definition 3.1. To examine Property (c1) take again $S' = H^n$ and $a_i = \mathrm{pr}_i : H^n \to H$. We have $\sigma^* K(a_1, \ldots, a_n) = K(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ and under (9.16) the isomorphism (9.11) corresponds to $\mathfrak{P}_\sigma$ (see (3.2)). Hence, we can see that Remark 9.3 (b) implies that ξ satisfies (c1) of Definition 3.1. It remains to discuss Property (c2). For this, we take $S' = H^{n+1}$ and $a_i = \mathrm{pr}_i : H^{n+1} \to H$, $0 \leq i \leq n$. Notice that we have

$$K(a_0, a_1, a_3, \ldots, a_n) *_2 K_{a_1}(a_0, a_2, \ldots, a_n) = K(a_0, a_1 + a_2, a_3, \ldots, a_n), \tag{9.17}$$

$$K(a_1, a_2, \ldots, a_n) *_1 K_{a_1}(a_0, a_2, \ldots, a_n) = K(a_0 + a_1, a_2, \ldots, a_n). \tag{9.18}$$

For example, when $n = 2$ these are explained by the following diagram of three "glued" squares

$$\begin{tikzcd}
a_2 \arrow[r, dash] \arrow[d, dash] & a_1 + a_2 \arrow[r, dash] \arrow[d, dash] & a_0 + a_1 + a_2 \arrow[d, dash] \\
0 \arrow[r, dash] & a_1 \arrow[r, dash] \arrow[d, dash] & a_0 + a_1 \arrow[d, dash] \\
 & 0 \arrow[r, dash] & a_0
\end{tikzcd} \tag{9.19}$$

(the general case is just harder to draw: Here the vertical glueing on the right corresponds to (9.17) while the horizontal to (9.18)). The relations (9.17), (9.18) together with (9.9) give isomorphisms

$$\delta((K(a_0, a_1, a_3, \ldots, a_n)) \otimes \delta((K_{a_1}(a_0, a_2, \ldots, a_n)) \simeq \delta((K(a_0, a_1 + a_2, a_3, \ldots, a_n)),$$
$$\delta((K(a_1, a_2, \ldots, a_n)) \otimes \delta((K_{a_1}(a_0, a_2, \ldots, a_n)) \simeq \delta((K(a_0 + a_1, a_2, \ldots, a_n)).$$

Combining these gives:

$$\delta^n(K(a_0 + a_1, a_2, \ldots, a_n)) \otimes \delta^n(K(a_0, a_1, a_3, \ldots, a_n)) \simeq$$
$$\simeq \delta^n(K(a_0, a_1 + a_2, a_3, \ldots, a_n)) \otimes \delta^n(K(a_1, a_2, \ldots, a_n)).$$

We can see, by using (9.16), that this isomorphism corresponds to $\mathfrak{Q}$ of (3.7). It now follows that the glueing condition on Ξ implies that the trivialization ξ respects the isomorphism $\mathfrak{Q}$. In other words, Property (c2) of Definition 3.1 is true for ξ. □

Remark 9.6. In fact, it is true that there is a bijective correspondence between n-cubic structures on the functor $\delta : H \to \mathcal{PIC}(S)$ in the sense of Definition 9.2 above and n-cubic structures on $\mathcal{L}_\delta$ in the sense of Definition 3.1: Assume that $\mathcal{L} = \mathcal{L}_\delta$ supports an n-cubic structure ξ in the sense of 3.1. In view of (9.16) the isomorphism ξ gives a functorial trivialization of $\delta^n(K(b_1, \ldots, b_n))$ for all points $b_1, \ldots, b_n$ of H. The relation (9.18) together with (9.9) give a canonical isomorphism

$$\delta^n(K_{b_0}(b_1, \ldots, b_n)) \simeq \delta^n(K(b_0 + b_1, \ldots, b_n)) \otimes \delta^n(K(b_0, b_2, \ldots, b_n))^{-1}. \tag{9.20}$$

We can now use (9.20) and the aforementioned trivialization of $\delta^n(K(b_1, \ldots, b_n))$ to define a functorial trivialization of $\delta^n(K_{b_0}(b_1, \ldots, b_n))$. One can verify that Properties (c0), (c1) and (c2) of Definition 3.1 imply that this trivialization of $\delta^n(K_{b_0}(b_1, \ldots, b_n))$ defines an n-cubic structure on δ. Since we are not going to use this statement we choose to omit the details.

9.e. Let $h : Y \to S$ be a projective and flat morphism of relative dimension d over the locally Noetherian scheme S. If $\mathcal{H}$ is a locally free coherent sheaf of $\mathcal{O}_Y$-modules on Y then the total derived image $\mathbf{R}h_*(\mathcal{H})$ in the derived category of complexes of sheaves of $\mathcal{O}_S$-modules which are bounded below is “perfect” (i.e it is locally on S quasi-isomorphic to a bounded complex of finitely generated free $\mathcal{O}_S$-modules, see [SGA6] III). Hence, by [KM], we can associate to $\mathbf{R}h_*(\mathcal{H})$ a graded invertible sheaf

$$\det{}_*\mathbf{R}h_* = (\det \mathbf{R}h_*(\mathcal{H}), \mathrm{rk}(\mathbf{R}h_*(\mathcal{H}))$$

on S (the “determinant of cohomology”). By restricting to $\mathcal{H}$ which are invertible, we obtain a functor, which we will denote again by $\det_* \mathbf{R}h_*$, from the Picard category of invertible sheaves on Y to the Picard category of graded invertible sheaves on S. In fact, by loc. cit. the formation of the determinant of cohomology commutes with arbitrary base changes $S' \to S$; hence we can define a corresponding S_{fppf}-functor

$$\det{}_*\mathbf{R}h_* : \mathcal{PIC}(Y) \to \mathcal{PIC}_*(S).$$

By the main result of [Du] (Theorem 4.2) this functor supports a canonical $d+2$-cubic structure (in the sense of [Du] Definition 1.6.1). Let us remark here that since $\mathcal{PIC}_*(S)$ is not strictly commutative we do have to refer to [Du] for the definition of cubic structure. (See Remark 9.3 (a).) Now observe that the substack $\mathcal{PIC}_{\mathrm{ev}}(S)$ of $\mathcal{PIC}_*(S)$ given by graded line bundles $(\mathcal{M}, e)$ with e always *even* is a s.c. Picard stack. The forgetful functor $f : \mathcal{PIC}_{\mathrm{ev}}(S) \to \mathcal{PIC}(S)$ is an additive functor. (Note that this is not true for the forgetful functor $\mathcal{PIC}_*(S) \to \mathcal{PIC}(S)$.) This fact together with [Du] Theorem 4.2 and Remark 9.3 (a) implies the following:

i) The functor $\mathcal{PIC}(Y) \to \mathcal{PIC}(S)$ given by $\mathcal{H} \mapsto \det \mathbf{R}h_*(\mathcal{H})^{\otimes 2}$ supports a canonical $d+2$-cubic structure in the sense of Definition 9.2.

ii) Let $\mathcal{PIC}^{\rm ev}(Y)$ be the substack of $\mathcal{PIC}(Y)$ given by invertible sheaves for which the function $\mathrm{rk}(\mathbf{R}h_*(\mathcal{H}))$ is always even. Then the functor $\mathcal{PIC}^{\rm ev}(Y) \to \mathcal{PIC}(S)$ given by $\mathcal{H} \mapsto \det \mathbf{R}h_*(\mathcal{H})$ supports a canonical $d+2$-cubic structure in the sense of Definition 9.2.

Remark 9.7. In fact, one can give a somewhat more direct proof of (i) and (ii) by following the general strategy of the proof of the main theorem of [Du]. The argument is considerably less involved since we do not have to deal with the thorny problem of signs that complicates the proof of [Du] Theorem 4.2.

9.f. Let $h : Y \to S$ be as in the previous paragraph and assume in addition that S is the spectrum of a Dedekind ring R with field of fractions K. Suppose that $\pi : X \to Y$ is a G-torsor with G a finite abelian group. The construction of §2.d gives an additive $S_{\rm fppf}$-functor

$$F : G^D_S \to \mathcal{PIC}(Y)\ ; \quad F(\chi) = \mathcal{O}_{X,\chi}. \tag{9.21}$$

Let $h_{G^D} : Y \times_S G^D_S \to G^D_S$ be the base change of $h : Y \to S$; we can view $\pi_*(\mathcal{O}_X)$ as an invertible sheaf on $Y \times_S G^D$ which is isomorphic to the value $\mathcal{O}_{X,\chi_0}$ of the functor F on the "universal" point $\chi_0 = \mathrm{id} : G^D_S \to G^D_S$ (see (2.7)). Now notice that the invertible $\mathcal{O}_{Y\times_S G^D}$-sheaf $\pi_*(\mathcal{O}_X)$ is $\#G$-torsion (this follows from (2.7) and (2.9)). Therefore, we have an equality of Euler characteristics (ranks)

$$\mathrm{rk}(\mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))) = \mathrm{rk}(\mathbf{R}h_{G^D *}(\mathcal{O}_{Y\times_S G^D_S})).$$

(For example, this equality can be deduced as follows: In the Grothendieck group $\mathrm{K}_0(Y \times_S G^D)$ of locally free coherent modules on $Y \times_S G^D$ the rank zero element $z = [\pi_*(\mathcal{O}_X)] - [\mathcal{O}_{Y\times_S G^D}]$ is nilpotent. Now since $\pi_*(\mathcal{O}_X)$ is a $\#G$-torsion invertible sheaf, it follows that a power of $\#G$ annihilates z. Hence, z has Euler characteristic equal to zero and this implies the equality.) Using the projection formula and the flatness of $Y \to S$, we see that the locally constant function $G^D_S \to \mathbf{Z}$ given by $\mathrm{rk}(\mathbf{R}h_{G^D *}(\mathcal{O}_{Y\times_S G^D_S}))$ always takes the value $\chi(Y, \mathcal{O}_Y) = \chi(Y_K, \mathcal{O}_{Y_K}) := \sum_i (-1)^i \mathrm{rk}_K \mathrm{H}^i(Y_K, \mathcal{O}_{Y_K})$. We can now conclude using base change that for any S'-valued point χ of G^D_S the function $\mathrm{rk}(\mathbf{R}h_{S' *}(\mathcal{O}_{X,\chi}))$ is constant with value $\chi(Y_K, \mathcal{O}_{Y_K})$. This value is even if and only if the arithmetic genus $g(Y_K) = (-1)^d(\chi(Y_K, \mathcal{O}_{Y_K}) - 1)$ of the generic fiber is odd.

Now let $\kappa = \gcd(2, g(Y_K))$ and consider the composition

$$\delta := \det \mathbf{R}h_*^{\otimes\kappa} \cdot F : G^D_S \to \mathcal{PIC}(S) \tag{9.22}$$

given by $\chi \mapsto \det \mathbf{R}h_*(\mathcal{O}_{X,\chi})^{\otimes\kappa}$. By Lemma 9.4 and (i), (ii) of §9.e above (applied when $g(Y_K)$ is even, odd respectively) we conclude that the functor δ has a canonical $d+2$-cubic structure in the sense of Definition 9.2. Using Lemma 9.5 and $\pi_*(\mathcal{O}_X) = \mathcal{O}_{X,\chi_0}$, we see that the $d+2$-cubic structure on δ equips the invertible sheaf $\mathcal{L}_\delta = \det \mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ over G^D_S with a corresponding $d+2$-cubic structure in the sense of Definition 3.1. We summarize:

Theorem 9.8. *Let $h : Y \to S$ be a projective and flat morphism of relative dimension d over the spectrum of a Dedekind ring with field of fractions K; set $\kappa = \gcd(2, g(Y_K))$*

with $g(Y_K) = (-1)^d(\chi(Y_K, \mathcal{O}_{Y_K}) - 1)$ the arithmetic genus of the generic fiber of $Y \to S$. Suppose that $\pi : X \to Y$ is a G-torsor for the finite abelian group G. Then the invertible sheaf $\det \mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ *over G^D_S supports a $d+2$-cubic structure.* □

Remark 9.9. The Taylor expansion formula (5.6) for $\mathcal{L} = \det \mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ (with its $d+2$-cubic structure provided by Theorem 9.8) closely resembles a Riemann-Roch formula "without denominators". To explain this, assume for simplicity that the morphism $h : Y \to S$ is smooth and that $\kappa = 1$. Let $\chi : G \to R'^*$ be a character of G with values in the Dedekind ring R' and consider the invertible sheaf $\mathcal{O}_{X,\chi}$ on $Y' = Y \times_R R'$. The Grothendieck-Riemann-Roch theorem for the morphism $h' : Y' \to S' = \mathrm{Spec}\,(R')$ gives

$$[\det \mathbf{R}h'_*(\mathcal{O}_{X,\chi})] = [\det \mathbf{R}h'_*(\mathcal{O}_{Y'})] + \sum_{i=0}^{d} h'_*\Big[\frac{c_1(\mathcal{O}_{X,\chi})^{d+1-i}}{(d+1-i)!} \cap \mathrm{Td}_i((\Omega^1_{Y/R})^*)\Big] \tag{9.23}$$

in $\mathrm{Pic}(S')_{\mathbf{Q}} = \mathrm{CH}^1(S')_{\mathbf{Q}}$ (see for example [Fa] Theorem 1.7 or [Fu] §15). Of course, this result is of little use since in our case of interest $\mathrm{Pic}(S')_{\mathbf{Q}} = \mathrm{Pic}(R') \otimes_{\mathbf{Z}} \mathbf{Q} = (0)$. Our point is that the Taylor expansion (5.6) provides a "without denominators" version of this equality. In fact, we can conjecture a precise relationship between the terms of (5.6) and those of (9.23): Let $\chi : S' \to G^D_S$ be the morphism given by the character χ. First of all, we have $\chi^*(\mathcal{L}) \simeq \det \mathbf{R}h'_*(\mathcal{O}_{Y,\chi})$, $\chi^*(0^*\mathcal{L}) \simeq \det \mathbf{R}h'_*(\mathcal{O}_{Y'})$. Let us consider the rest of the terms. The standard formula for the Todd class gives a (universal) expression $\mathrm{Td}_i((\Omega^1_{Y'/R'})^*) = N_i \cdot T_i$ with $N_i \in \mathbf{Q}$, T_i an integral linear combination of Chern classes of $\Omega^1_{Y'/R'}$ in $\mathrm{CH}^i(Y')$ ($N_0 = 1$, $N_1 = 1/2$, $N_2 = 1/12$, $N_3 = 1/24$, $N_4 = 1/720$; in general N_i is given using Bernoulli numbers). We conjecture that for all $i = 0, \ldots, d$

$$[\chi^*(\delta(\mathcal{L}^{(i)}, \xi^{(i)})] = (-1)^i \frac{(d+1)!!N_i}{(d-i)!!(d+1-i)!} h'_*\Big[c_1(\mathcal{O}_{X,\chi})^{d+1-i} \cap T_i\Big] \tag{9.24}$$

in $\mathrm{Pic}(S')$. (It follows from the theorem of von Staudt-Clausen -[Wa] Theorem 5.10- that this coefficient is integral.) In the case of arithmetic surfaces ($d = 1$), this conjecture follows from the Deligne-Riemann-Roch theorem ([De] (7.5.1)). In fact, in this case we can see that $\delta(\mathcal{L}^{(0)}, \xi^{(0)}) \simeq <\pi_*(\mathcal{O}_X), \pi_*(\mathcal{O}_X)>$, $\delta(\mathcal{L}^{(1)}, \xi^{(1)}) \simeq <\pi_*(\mathcal{O}_X), \omega_{Y\times_S G^D_S/G^D_S}>$ (notations as in loc. cit.) and that the Taylor expansion (5.6) amounts to the Deligne-Riemann-Roch formula. We will leave the details for another occasion.

10. The multiextension associated to a $\mathbf{Z}/p$-torsor.

In this section, we assume that $G = \mathbf{Z}/p$, p a prime, and that $\pi : X \to Y$ is a G-torsor with $Y \to S = \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d. In addition, we will assume that the generic fiber $Y_{\mathbf{Q}}$ is normal. By Theorem 9.8 the line bundle $\mathcal{L}_\delta = \det \mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ on G^D is equipped with a canonical $d+2$-cubic structure ξ. We will now give a rather explicit description of the isomorphism class of the corresponding

(via the construction of §5.a) $d+1$-extension $E(\mathcal{L}_\delta, \xi)$ on $\Theta_{d+1}(\mathcal{L}_\delta)$. Using Remark 7.13 we see that it is enough to describe the image of the class of $E(\mathcal{L}_\delta, \xi)$ under the homomorphism

$$d+1\text{-}\mathrm{Ext}^1(\mu_p, \mathbf{G}_m) \xrightarrow{\psi'_{d+1}} \mathrm{H}^1(\mu_p, \mathbf{Z}/p) \hookrightarrow \mathrm{H}^1(\mathrm{Spec}\,(\mathbf{Q}(\zeta_p)), \mathbf{Z}/p), \tag{10.1}$$

where the second arrow is given by restriction along the generic point $\mathrm{Spec}\,(\mathbf{Q}(\zeta_p)) \to \mu_p$. Now set $U = X_{\mathbf{Q}(\zeta_p)}$, $V = Y_{\mathbf{Q}(\zeta_p)}$. Then $U \to V$ is a G-torsor of normal projective schemes of dimension d over $\mathbf{Q}(\zeta_p)$. Consider the character $\chi_0 : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Q}(\zeta_p)^*$ given by $\chi_0(1) = \zeta_p$. By §2.d, the χ_0-isotypic part $\mathcal{O}_{U,\chi_0}$ of the $\mathcal{O}_V$-sheaf $\pi_*(\mathcal{O}_U)$ is an invertible sheaf on V which is p-torsion. Let A be a generic section of this invertible sheaf; A is then an element of the function field $k(U)$ and $a \in \mathbf{Z}/p$ acts on it by multiplication by $\chi_0(a) = \zeta_p^a$. Hence, $F = A^p$ belongs to the function field $k(V)$. Using the section A we can associate to the invertible sheaf $\mathcal{O}_{U,\chi_0}$ a Cartier divisor D on V. We can see that $p \cdot D$ is equal to the principal Cartier divisor (F).

Consider the group $Z_0(V)$ of 0-cycles on V and the Chow group $A_0(V)$ of 0-cycles on V modulo rational equivalence (see [Fu], 2.4). Suppose that P is a closed point of V with residue field $k(P)$ (a finite extension of $\mathbf{Q}(\zeta_p)$). Specializing the cover $U \to V$ at P_i gives a G-torsor over $\mathrm{Spec}\,(k(P))$ which, by Kummer theory (Remark 2.3), corresponds to $f \in k(P)^*/(k(P)^*)^p$. Set $\lambda(P) = \mathrm{Norm}_{k(P)/\mathbf{Q}(\zeta_p)}(f) \in \mathbf{Q}(\zeta_p)^*/(\mathbf{Q}(\zeta_p)^*)^p$. By extending linearly we obtain a group homomorphism

$$\lambda : Z_0(V) \to \mathbf{Q}(\zeta_p)^*/(\mathbf{Q}(\zeta_p)^*)^p.$$

Lemma 10.1. *The homomorphism a factors through rational equivalence and provides us with a group homomorphism*

$$\lambda : A_0(V) \to \mathbf{Q}(\zeta_p)^*/(\mathbf{Q}(\zeta_p)^*)^p \ .$$

PROOF. Consider two 0-cycles Z, Z' which are rationally equivalent. By definition, there is then a projective reduced curve $C \subset V$ passing through all points in the supports of Z and Z' and a function ϕ on the normalization $q : \tilde{C} \to C$ such that $q_*((\phi)) = Z - Z'$ where the push-forward q_* of the divisor (ϕ) by q is defined as in [Fu] 1.4. A standard moving argument, shows that we can choose a generic section A of $\mathcal{O}_{U,\chi_0}$ as above, such that the divisor of $F = A^p$ is disjoint from all the points in the supports of Z and Z' and from the generic points of C. Specializing F on C gives an element f in the function algebra (the product of the function fields of the irreducible components) $k(C) = k(\tilde{C})$. Now if Q is a point of C (resp. of $\tilde{C}$) which is not in the support of $q_*((f))$ (resp. of (f)) then we denote by $f(Q)$ the Norm from $k(Q)$ to $\mathbf{Q}(\zeta_p)$ of the "evaluation" of f at Q. Extending by linearity, we can make sense of $f(Z)$ and $f(Z')$. By our choice of f, we have

$$\lambda(Z) = f(Z) \bmod (\mathbf{Q}(\zeta_p)^*)^p, \qquad \lambda(Z') = f(Z') \bmod (\mathbf{Q}(\zeta_p)^*)^p,$$

(see Remark 2.3 (a)) and therefore $\lambda(Z) \cdot \lambda(Z')^{-1} = f(q_*((\phi))) \bmod (\mathbf{Q}(\zeta_p)^*)^p$. By the definitions of q_* and $f(-)$ we now obtain that $f(q_*((\phi))) = f((\phi))$ where in the second expression f (resp. (ϕ)) is regarded as a function (resp. a divisor) on the smooth projective

curve $\tilde{C}$. By Weil reciprocity on $\tilde{C}$, $f((\phi)) = \phi((f))$. Now observe that the divisor (f) on $\tilde{C}$ is the p-th multiple of the pull back of the Cartier divisor D via $\tilde{C} \to V$. Therefore, $f(q_*((\phi))) = \phi((f))$ is in $(\mathbf{Q}(\zeta_p)^*)^p$ and this completes the proof. □

Remark 10.2. The homomorphism λ is closely connected to the cohomological Abel-Jacobi map described in [C-TS]. For simplicity, set $K = \mathbf{Q}(\zeta_p)$. Following Bloch, Colliot-Thélène and Sansuc construct a "characteristic homomorphism"

$$\Phi : A_0(V) \to \mathrm{Ext}^1_{\mathrm{Gal}(\bar{K}/K)}(\mathrm{Pic}(V_{\bar{K}}), \bar{K}^*) \tag{10.2}$$

(extensions of discrete $\mathrm{Gal}(\bar{K}/K)$-modules). One can see from their construction that pulling back along $\mathbf{Z}/p \to \mathrm{Pic}(V_{\bar{K}})$ given by $1 \mapsto D$, and composing with the isomorphism $\mathrm{Ext}^1_{\mathrm{Gal}(\bar{K}/K)}(\mathbf{Z}/p, \bar{K}^*) \simeq K^*/(K^*)^p$ given by Hilbert's Theorem 90 gives the homomorphism λ above.

Since D is a Cartier divisor, the d-th self intersection $D^d := D \cap \cdots \cap D$ makes sense as an element of the Chow group $A_0(V)$ (see [Fu], 2.4) and we can set

$$\lambda(X/Y) = \lambda(D^d)\ .$$

Recall $\kappa = \gcd(2, g(Y_{\mathbf{Q}}))$.

Proposition 10.3. *Set* $L = \mathbf{Q}(\zeta_p)[y]/(y^p - \lambda(X/Y)^{-\kappa})$*; then* $T(X/Y) = \mathrm{Spec}\,(L)$ *is a* $\mathbf{Z}/p$*-torsor over* $\mathrm{Spec}\,(\mathbf{Q}(\zeta_p))$ *whose class in* $\mathrm{H}^1(\mathrm{Spec}\,(\mathbf{Q}(\zeta_p)), \mathbf{Z}/p)$ *is the image of the isomorphism class of the* $d+1$*-extension* $E(\mathcal{L}_\delta, \xi)$ *under the injective map (10.1).*

Proof. For simplicity, let us denote by $E(X/Y)$ the multiextension $E(\mathcal{L}_\delta, \xi)$ associated to the torsor $X \to Y$. Consider the base change of the multiextension $E(X/Y)$ by the morphism $\mathrm{Spec}\,(\mathbf{Q}) \to S = \mathrm{Spec}\,(\mathbf{Z})$. This is isomorphic to the multiextension $E(X_{\mathbf{Q}}/Y_{\mathbf{Q}})$ associated to the torsor $X_{\mathbf{Q}} \to Y_{\mathbf{Q}}$. Let τ be the image of the isomorphism class of $E(X_{\mathbf{Q}}/Y_{\mathbf{Q}})$ under the map

$$d+1\text{-}\mathrm{Ext}^1(\mu_{p_{/\mathbf{Q}}}, \mathbf{G}_{m/\mathbf{Q}}) \xrightarrow{\psi'_{d+1}} \mathrm{H}^1(\mu_{p_{/\mathbf{Q}}}, \mathbf{Z}/p) \to \mathrm{H}^1(\mathrm{Spec}\,(\mathbf{Q}(\zeta_p)), \mathbf{Z}/p). \tag{10.3}$$

(Here $\mu_{p_{/\mathbf{Q}}}$, $\mathbf{G}_{m/\mathbf{Q}}$ is short hand notation for the group schemes $\mu_p \times_S \mathrm{Spec}\,(\mathbf{Q})$, $\mathbf{G}_m \times_S \mathrm{Spec}\,(\mathbf{Q})$ over $\mathrm{Spec}\,(\mathbf{Q})$. The first arrow is defined by the construction of (7.16) performed over the base $\mathrm{Spec}\,(\mathbf{Q})$.) We can see that it is enough to show that the class of $T(X/Y)$ is equal to the image τ. By unraveling the definition of ψ'_{d+1} (Remark 7.13) we can now see that the torsor class τ corresponds (under the "Waterhouse isomorphism" (6.13)) to the $\mathbf{G}_m \times_S \mathrm{Spec}\,(\mathbf{Q}(\zeta_p))$-extension over $\mu_p \times_S \mathrm{Spec}\,(\mathbf{Q}(\zeta_p))$ given by the additive functor on characters of $\mathbf{Z}/p$

$$\chi \mapsto E(X_{\mathbf{Q}}/Y_{\mathbf{Q}})_{(\chi_0, \ldots, \chi_0, \chi)} \tag{10.4}$$

(see §4.a). According to the definition of $E(X_{\mathbf{Q}}/Y_{\mathbf{Q}})$,

$$E(X_{\mathbf{Q}}/Y_{\mathbf{Q}})_{(\chi_0, \ldots, \chi_0, \chi)} = \bigotimes_{k=0}^{d+1} \Bigg(\bigotimes_{i_1 < \cdots < i_k} (\det \mathbf{R} h'_*(\mathcal{O}_{U, \chi[i_1]} \otimes \cdots \otimes \mathcal{O}_{U, \chi[i_k]}))^{\otimes \kappa} \Bigg)^{(-1)^{d+1-k}}$$

with $\chi[i]=\chi_0$ if $i\neq d+1$, $\chi[d+1]=\chi$, and $h': V\to \mathrm{Spec}\,(\mathbf{Q}(\zeta_p))$ the structure morphism. In fact, we can view the right hand side of the above equality as a value of the "intersection sheaf" ([De] or [Du] §5): If $\mathcal{L}_i$, $i=1,\ldots,d+1$, are invertible sheaves on V, then by definition

$$I(\mathcal{L}_1,\ldots,\mathcal{L}_{d+1}) := \bigotimes_{k=0}^{d+1}\Bigg(\bigotimes_{i_1<\cdots<i_k} \det\mathbf{R}h'_*(\mathcal{L}_{i_1}\otimes\cdots\otimes\mathcal{L}_{i_k})\Bigg)^{(-1)^{d+1-k}}, \tag{10.5}$$

and so

$$E(X_{\mathbf{Q}}/Y_{\mathbf{Q}})_{(\chi_0,\ldots,\chi_0,\chi)} = I(\mathcal{O}_{U,\chi_0},\ldots,\mathcal{O}_{U,\chi_0},\mathcal{O}_{U,\chi})^{\otimes\kappa}. \tag{10.6}$$

Now let us return to the notations before the statement of the Proposition. A standard argument shows that we can write $\mathcal{O}_{U,\chi_0}=\mathcal{M}_1\otimes\mathcal{M}_2^{-1}$ with $\mathcal{M}_i$ very ample invertible sheaves on V that have sections s_1^j and s_2^j, $j=1,\ldots,d$, respectively, with the following property: All sequences $(\underline{s})$ of the form $(s^1_{i_1},s^2_{i_2},\ldots,s^d_{i_d})$, for $i_1,\ldots,i_d\in\{1,2\}$ are regular. (By definition, this means that the corresponding sequences of elements of the local rings $\mathcal{O}_{V,x}$, $x\in V$, which are obtained from the s_i^j using local trivializations of $\mathcal{M}_i$ are regular.) Let us denote by $w(\underline{s})$ the number of indices $j=1,\ldots,d$ in the sequence $(\underline{s})$ where the subscript is equal to 2. For each such sequence $(\underline{s})$, the scheme theoretic intersection $Z_{(\underline{s})}=\mathrm{div}(s^1_{i_1})\cap\mathrm{div}(s^2_{i_2})\cap\cdots\cap\mathrm{div}(s^d_{i_d})$ is a union of reduced closed points of V and we have

$$\sum_{(\underline{s})}(-1)^{w(\underline{s})}[Z_{(\underline{s})}] = D^d \tag{10.7}$$

in the Chow group $A_0(V)$. Using the additivity and restriction properties of the intersection sheaves ([Du] §5, [De]) and (10.6) we can see that the functor (10.4) is isomorphic (as an additive functor) to the functor

$$\chi\mapsto \bigotimes_{(\underline{s})}\mathrm{Norm}_{Z_{(\underline{s})}/\mathrm{Spec}\,(\mathbf{Q}(\zeta_p))}(\mathcal{O}_{U,\chi}|_{Z_{(\underline{s})}})^{\otimes(-1)^{w(\underline{s})}\cdot\kappa}\ . \tag{10.8}$$

We have a natural isomorphism $\mathcal{O}_{U,\chi_0}|_{Z_{(\underline{s})}}\simeq\mathcal{O}_{\pi^{-1}(Z_{(\underline{s})}),\chi_0}$ where $\pi^{-1}(Z_{(\underline{s})})\to Z_{(\underline{s})}$ is the $\mathbf{Z}/p$-torsor obtained by base changing $\pi_{\mathbf{Q}}: X_{\mathbf{Q}}\to Y_{\mathbf{Q}}$ along $Z_{(\underline{s})}\to Y_{\mathbf{Q}}$. We can now see that, under the description of Remark 2.3 (a), the $\mathbf{Z}/p$-torsor τ is given by the invertible sheaf

$$\bigotimes_{(\underline{s})}\mathrm{Norm}_{Z_{(\underline{s})}/\mathrm{Spec}\,(\mathbf{Q}(\zeta_p))}(\mathcal{O}_{\pi^{-1}(Z_{(\underline{s})}),\chi_0^{-1}})^{\otimes(-1)^{w(\underline{s})}\cdot\kappa}$$

together with the natural trivialization of its p-th power induced by the isomorphism $\mathcal{O}^{\otimes p}_{U,\chi_0^{-1}}\simeq\mathcal{O}_V$ and the additivity of the norm. (Recall that the $\mathbf{Z}/p$-torsor τ corresponds –under (6.13)– to the extensions given by the additive functors (10.4) and (10.8). The inverse χ_0^{-1} in the expression above occurs, instead of χ_0, because of Remark 6.2 (a)). It now follows from Remark 2.3 (b) that a Kummer element for this $\mathbf{Z}/p$-torsor over $\mathrm{Spec}\,(\mathbf{Q}(\zeta_p))$ is given by taking the inverse of the product over all $(\underline{s})$ of the Norms from $Z_{(\underline{s})}$ to $\mathrm{Spec}\,(\mathbf{Q}(\zeta_p))$ of Kummer elements for the $\mathbf{Z}/p$-torsors $\pi^{-1}(Z_{(\underline{s})})\to Z_{(\underline{s})}$. Hence, the result now follows from (10.7) and Lemma 10.1. □

Remark 10.4. Assume that $p > d+1$.

a) Proposition 10.3 gives an explicit description of the $\mathbf{Z}/p$-extension of $\mathbf{Q}(\zeta_p)$ that corresponds via class field theory to the element $t_{d+1}(\mathcal{L},\xi) \in \mathrm{Hom}(C(p), \mathbf{Z}/p)$ (defined in the section §8.d) when $(\mathcal{L},\xi)$ is given by $\det \mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ with its canonical cubic structure. Indeed, we can see that the class of the $\mathbf{Z}/p$-extension that corresponds to $t_{d+1}(\mathcal{L},\xi)$ is equal to $\frac{1}{(d+1)!}(T(X/Y))$ in $\mathrm{H}^1(\mathrm{Spec}\,(\mathbf{Q}(\zeta_p), \mathbf{Z}/p)$.

b) We conjecture that the elements $\{t_{d+1}(\mathcal{L},\xi)\}$, $X \to Y$ ranging over all $\mathbf{Z}/p\mathbf{Z}$-torsors with $Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d, generate the target group $\mathrm{Hom}((C/p)^{(-d)}, \mathbf{Z}/p\mathbf{Z})$. To this moment we have no direct evidence to support this conjecture. Any calculation proves to be quite difficult: Indeed, the lowest dimension for which the group $\mathrm{Hom}((C/p)^{(-d)}, \mathbf{Z}/p\mathbf{Z})$ is non-trivial for $p < 12\cdot 10^6$ is $d = 11$; then we have a non-trivial group for $p = 691$. On the other hand, it is easier to examine analogous statements over bases more general than $\mathrm{Spec}\,(\mathbf{Z})$; some (indirect) evidence can be collected this way. We intend to return to this topic in a subsequent paper.

c) Suppose $d \geq 2$, the generic fibers $X_{\mathbf{Q}}$, $Y_{\mathbf{Q}}$ are smooth and the p-torsion divisor D on $V = Y_{\mathbf{Q}(\zeta_p)}$ is algebraically equivalent to zero, i.e corresponds to a p-torsion point in the Picard variety $\mathrm{Pic}^0(V)$. Then $t_{d+1}(\mathcal{L},\xi) = 0$. (Therefore examples of non-trivial elements $t_{d+1}(\mathcal{L},\xi)$ can only come from p-torsion in the Neron-Severi group of V.) Let us quickly sketch a proof of this fact. (Here we will give a straightforward argument. Later, in the course of the proof of Theorem 1.3, we will show a stronger result; see Remark 11.8). Notice that we have a commutative diagram

$$\begin{array}{ccc} (A_0(V))_{\mathrm{degree}=0} & \xrightarrow{\Phi} & \mathrm{Ext}^1_{\mathrm{Gal}(\bar{K}/K)}(\mathrm{Pic}(V_{\bar{K}}), \bar{K}^*) \\ \downarrow & & \downarrow \\ \mathrm{Alb}(V)(K) & \xrightarrow{\Phi} & \mathrm{Ext}^1_{\mathrm{Gal}(\bar{K}/K)}(\mathrm{Pic}^0(V_{\bar{K}}), \bar{K}^*). \end{array} \tag{10.9}$$

Here $K = \mathbf{Q}(\zeta_p)$, $\mathrm{Alb}(V)$ is the Albanese variety of V and Φ is the homomorphism of [C-TS] as in Remark 10.2. Using that remark and the above, we can see that the homomorphism $\lambda : (A_0(V))_{\mathrm{degree}=0} \to K^*/(K^*)^p$ factors through $(A_0(V))_{\mathrm{degree}=0} \to \mathrm{Alb}(V)(K) \to K^*/(K^*)^p$. Using Proposition 10.3, we now see that to show $t_{d+1}(\mathcal{L},\xi) = 0$ is enough to show that the self-intersection $D^d \in (A_0(V))_{\mathrm{degree}=0}$ has trivial image in $\mathrm{Alb}(V)(K)$. It is enough to show that the corresponding p-torsion point of $\mathrm{Alb}(V)(K)$ is trivial in $\mathrm{Alb}(V)(k(\mathfrak{P})) \subset \mathrm{Alb}(V)(\overline{k(\mathfrak{P})})$ (that is after reduction modulo some prime $\mathfrak{P}$ of K that does not divide p and where V has good reduction; her $k(\mathfrak{P})$ is the residue field of $\mathfrak{P}$). In this case intersections commute with specialization, and so this reduction is obtained as the image of the d-th self-intersection $\bar{D}^d \in A_0(V_{\overline{k(\mathfrak{P})}})$ of $\bar{D} \in \mathrm{Pic}^0(V_{\overline{k(\mathfrak{P})}})$. However $\bar{D}$ is a torsion element in a divisible group and the intersection pairing is bilinear. It follows that $\bar{D}^d = 0$ in $A_0(V_{\overline{k(\mathfrak{P})}})$.

Remark 10.5. Our construction in this paragraph actually gives a map

$$\mathrm{H}^1(Y_{\mathbf{Q}}, \mathbf{Z}/p) \longrightarrow \mathbf{Q}(\zeta_p)^*/(\mathbf{Q}(\zeta_p)^*)^p = \mathrm{H}^1(\mathbf{Q}(\zeta_p), \mathbf{Z}/p).$$

It is not hard to see that this map is a group homomorphism. When $h_{\mathbf{Q}} : Y_{\mathbf{Q}} \to \mathrm{Spec}\,(\mathbf{Q})$ is smooth it can also be derived from étale duality for the smooth projective morphism $h_{\mathbf{Q}}$. We will leave the details to the interested reader.

11. Galois module structure

In this section, we complete the proofs of the main results stated in the introduction. We begin with some preliminaries.

11.a. Let B be an associative ring with unit, which we assume is left Noetherian. Most of the time we will take B to be the group ring $R[G]$ of a finite group G with R commutative Noetherian. We denote by $\mathrm{G}_0(B)$ (resp. $\mathrm{K}_0(B)$) the Grothendieck group of finitely generated (resp. finitely generated projective) left B-modules, and by $\mathrm{G}_0^{\mathrm{red}}(B)$, resp. $\mathrm{K}_0^{\mathrm{red}}(B)$, the quotient of $\mathrm{G}_0(B)$, resp. $\mathrm{K}_0(B)$, by the subgroup generated by the class $[B]$ of the free B-module B. We will denote by a^{red} the image of the element a of $\mathrm{G}_0(B)$, resp. $\mathrm{K}_0(B)$, in $\mathrm{G}_0^{\mathrm{red}}(B)$, resp. $\mathrm{K}_0^{\mathrm{red}}(B)$. Denote by $c : \mathrm{K}_0(B) \to \mathrm{G}_0(B)$, $c^{\mathrm{red}} : \mathrm{K}_0^{\mathrm{red}}(B) \to \mathrm{G}_0^{\mathrm{red}}(B)$, the natural forgetful homomorphisms. If B is commutative, we will denote by $\mathrm{Pic}(B)$ the Picard group of B. If B is commutative, a finitely generated B-module is projective if and only if it is locally free. Taking highest exterior powers of locally free B-modules defines in this case a group homomorphism

$$i : \mathrm{K}_0^{\mathrm{red}}(B) \to \mathrm{Pic}(B).$$

We will denote by $D^+(B)$ the derived category of the homotopy category of complexes of left B-modules which are bounded below. Recall that a complex $C^\bullet$ in $D^+(B)$ is called "perfect", if it is isomorphic in $D^+(B)$ to a bounded complex $P^\bullet$ of finitely generated projective left B-modules. Then the element

$$\chi(C^\bullet) = \sum_i (-1)^i [P^i] \in \mathrm{K}_0(B) \tag{11.1}$$

depends only on the isomorphism class of $C^\bullet$ in $D^+(B)$.

In what follows, all the schemes will be separated and Noetherian. For a scheme Y, we will denote by $\mathrm{G}_0(Y)$, resp. $\mathrm{K}_0(Y)$, the Grothendieck group of coherent, resp. coherent locally free, sheaves of $\mathcal{O}_Y$-modules, and by $\mathrm{Pic}(Y)$ the Picard group of Y. If Y is regular and has an ample invertible sheaf, then we have $\mathrm{K}_0(Y) \simeq \mathrm{G}_0(Y)$ ([SGA6] IV). If $Y = \mathrm{Spec}\,(B)$ is affine, we will identify quasi-coherent sheaves of $\mathcal{O}_Y$-modules on Y with B-modules. This gives natural identifications $\mathrm{G}_0(B) = \mathrm{G}_0(\mathrm{Spec}\,(B))$, $\mathrm{K}_0(B) = \mathrm{K}_0(\mathrm{Spec}\,(B))$ and $\mathrm{Pic}(B) = \mathrm{Pic}(\mathrm{Spec}\,(B))$.

11.b. Now suppose that $S = \mathrm{Spec}\,(R)$, R regular Noetherian and that $\pi : X \to Y$ is a (right) torsor for a finite group G with $h : Y \to S$ projective. Then $f := \pi \cdot h : X \to S$ is also projective with a free (right) G-action. Denote by $\mathrm{G}_0(G, X)$, resp. $\mathrm{K}_0(G, X)$, the

Grothendieck group of G-equivariant coherent, resp. locally free coherent, sheaves on X. By descent (see §2.c) pulling back along the finite étale morphism π gives isomorphisms

$$\pi^*: \mathrm{G}_0(Y) \xrightarrow{\sim} \mathrm{G}_0(G,X), \quad \pi^*: \mathrm{K}_0(Y) \xrightarrow{\sim} \mathrm{K}_0(G,X). \tag{11.2}$$

Recall also (cf. §2.c) that if $\mathcal{F}$ is a G-equivariant coherent sheaf on X we can view $\pi_*(\mathcal{F})$ as a coherent sheaf of $\mathcal{O}_Y[G]$-modules on Y: If $V = \mathrm{Spec}\,(C)$ is an open affine subscheme of Y and $U = \pi^{-1}(V)$, then the sections $(\pi_*(\mathcal{F}))(V) = \mathcal{F}(U)$ are naturally a left $C[G]$-module. We can then consider the right derived image $\mathbf{R}\Gamma(Y, \pi_*(\mathcal{F}))$; this is a complex in $D^+(R[G])$ which computes the cohomology of $\pi_*(\mathcal{F})$ ([SGA6] III §2, IV §2). We may give a complex isomorphic to $\mathbf{R}\Gamma(Y, \pi_*(\mathcal{F}))$ by taking the (bounded) Čech complex obtained by considering the sections of $\pi_*(\mathcal{F})$ on the intersections of the sets in a finite affine cover $\{V_i\}_i$ of Y.

Theorem 11.1. *([CEPT1] Theorem 8.3; see also [C], [CE].) Assume as above that $\pi: X \to Y$ is a G-torsor, $h: Y \to S$ projective and $S = \mathrm{Spec}\,(R)$ is regular Noetherian. Let $\mathcal{F}$ be a G-equivariant coherent sheaf on X. Then the complex $\mathbf{R}\Gamma(Y, \pi_*(\mathcal{F}))$ in $D^+(R[G])$ is perfect. The elements*

$$\chi_f^P(\mathcal{F}) := \chi(\mathbf{R}\Gamma(Y, \pi_*(\mathcal{F}))) \in \mathrm{K}_0(R[G])$$

define a group homomorphism (the equivariant projective Euler characteristic)

$$\chi_f^P : \mathrm{G}_0(G,X) \to \mathrm{K}_0(R[G]).$$

We also set $\bar{\chi}_f^P(\mathcal{F}) := (\chi_f^P(\mathcal{F}))^{\mathrm{red}} \in \mathrm{K}_0^{\mathrm{red}}(R[G])$. Note that $\bar{\chi}_f^P(\mathcal{F}) \in \mathrm{K}_0^{\mathrm{red}}(R[G])$ is the obstruction for the complex $\mathbf{R}\Gamma(Y, \pi_*(\mathcal{F}))$ to be isomorphic in $D^+(R[G])$ to a bounded complex of finitely generated *free* $R[G]$-modules. When $f: X \to S$ is fixed, we will usually write χ^P, $\bar{\chi}^P$ instead of χ_f^P, $\bar{\chi}_f^P$.

Suppose now that R is the ring of integers of a number field. We will say that a $R[G]$-module M is locally free if for each prime ideal $\mathcal{P}$ of R, $M \otimes_R R_{\mathcal{P}}$ is a free $R_{\mathcal{P}}[G]$-module. By a theorem of Swan the notions of projective and locally free coincide for finitely generated $R[G]$-modules ([Sw]). Therefore, we may identify $\mathrm{K}_0^{\mathrm{red}}(R[G])$ with the class group of finitely generated locally free $R[G]$-modules and write $\mathrm{Cl}(R[G])$ instead of $\mathrm{K}_0^{\mathrm{red}}(R[G])$. Also, let us mention that in this case, χ_f^P coincides with the homomorphism $f_*^{CT}: \mathrm{G}_0(G,X) \to \mathrm{CT}(R[G]) = \mathrm{K}_0(R[G])$ of [C] and [CE] (here $\mathrm{CT}(R[G])$ denotes the Grothendieck group of finitely generated $R[G]$-modules which are cohomologically trivial as G-modules; see [C] and [CEPT1] Lemma 8.5).

11.c. In what follows, we continue with the general assumptions and notations of the previous paragraph. In addition, we will assume that G is commutative and that the morphisms $f: X \to S$ and $h: Y = X/G \to S$ are flat. We denote by $h_{G^D_S}: Y \times_S G^D_S \to G^D_S$ the base change of h. In what follows, we will omit the subscript S from G^D_S. The morphism h_{G^D} is also flat and projective. For any coherent sheaf $\mathcal{H}$ of $\mathcal{O}_{Y \times_S G^D}$-modules on $Y \times_S G^D$, we can consider the complex $\mathbf{R}h_{G^D *}(\mathcal{H})$ in the derived category $D^+(\mathcal{O}_{G^D})$ of the homotopy category of complexes of sheaves of $\mathcal{O}_{G^D}$-modules on G^D which are bounded below. In fact, if $\mathcal{H}$ is locally free, then $\mathbf{R}h_{G^D *}(\mathcal{H})$ is perfect ([SGA6] III)

and we can consider the determinant of cohomology $\det \mathbf{R}h_{G^D*}(\mathcal{H})$ (see §9.e) and the Euler characteristic $\chi(\mathbf{R}h_{G^D*}(\mathcal{H})) \in \mathrm{K}_0(R[G])$. (Notice that, by [KM] Prop. 4, over the affine scheme G^D, a complex is perfect in the sense of [SGA6] if and only if it is *globally* quasi-isomorphic to a bounded complex of sheaves associated to finitely generated locally free $R[G]$-modules; this allows us to define $\chi(\mathbf{R}h_{G^D*}(\mathcal{H})) \in \mathrm{K}_0(R[G])$ by a formula similar to (11.1).)

As in §2.d we may think of the locally free coherent sheaf $\pi_*(\mathcal{O}_X)$ of $\mathcal{O}_Y[G]$-modules on Y as an invertible sheaf of $\mathcal{O}_{Y\times_S G^D}$-modules on $Y\times_S G^D$. We can construct a bounded complex isomorphic to $\mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))$ by using the Čech construction associated to $\pi_*(\mathcal{O}_X)$ and the finite affine cover $\{V_i\times_S G^D\}_i$ of $Y\times_S G^D$, where $\{V_i\}_i$ is a finite affine cover of Y. It follows that the complexes $\mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))$ and $\mathbf{R}\Gamma(Y,\pi_*(\mathcal{O}_X))$ (see §11.b) are isomorphic (here again we identify $R[G]$-modules with the corresponding $\mathcal{O}_{G^D}$-sheaves). Both complexes $\mathbf{R}\Gamma(Y,\pi_*(\mathcal{O}_X))$ and $\mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))$ are perfect (by Theorem 11.1 and [SGA6] III). We obtain

$$i(\chi(\mathbf{R}\Gamma(Y,\pi_*(\mathcal{O}_X)))^{\mathrm{red}}) = [\det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))] \in \mathrm{Pic}(G^D_S) = \mathrm{Pic}(R[G])$$

and therefore

$$i(\bar{\chi}^P_f(\mathcal{O}_X)) = [\det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))]. \tag{11.3}$$

If R is of Krull dimension 1, which is the main case we are interested in, the same is true for $R[G]$. Then by [BM] Cor. 3.5, $i : \mathrm{K}_0^{\mathrm{red}}(R[G]) \to \mathrm{Pic}(R[G]) = \mathrm{Pic}(G^D_S)$ is an isomorphism. In this case, we will use i to identify the two groups; this should not cause any confusion. We can then write

$$\bar{\chi}^P_f(\mathcal{O}_X) = [\det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))]. \tag{11.4}$$

11.d. We continue with the general assumptions of the previous paragraph. In particular, G is a commutative group and $\pi : X \to Y$ is a G-torsor with $h : Y \to S = \mathrm{Spec}\,(R)$ projective and flat (R is regular and Noetherian). Recall that in this case, $\pi_*(\mathcal{O}_X)$ is an invertible sheaf over $Y\times_S G^D$ (§2.d). The corresponding $\mathbf{G}_m$-torsor supports a commutative extension

$$1 \to \mathbf{G}_{mY} \to E \to G^D_Y \to 1 \tag{11.5}$$

of group schemes over Y (see Remark 2.2).

Definition 11.2. *We will say that the G-torsor $\pi : X \to Y$ is of Albanese type over S if there is a smooth commutative group scheme of finite type $A \to S$ with connected fibers, a commutative extension*

$$1 \to \mathbf{G}_{mY} \to \mathcal{E} \to A_Y \to 1 \tag{11.6}$$

of group schemes over Y and a group scheme homomorphism $\phi : G^D_S \to A$ over S such that $E \simeq (\mathrm{id}_Y \times_S \phi)^*(\mathcal{E})$ as group scheme extensions.

Remark 11.3. a) If $\mathcal{P}$ is the invertible sheaf over $A_Y = Y \times_S A$ which corresponds to the $\mathbf{G}_{mY}$-torsor $\mathcal{E}$, then our condition implies that $\pi_*(\mathcal{O}_X) \simeq (\mathrm{id}_Y \times_S \phi)^*(\mathcal{P})$ as invertible shaves on G_Y^D.

b) Let $\pi : X \to Y$ be a G-torsor of Albanese type and suppose that $i : Z \to Y$ is a projective morphism such that $h \cdot i : Z \to S$ is flat. Then the G-torsor $\pi_Z : X \times_Y Z \to Z$ obtained by base change is also of Albanese type.

c) Suppose $S = \mathrm{Spec}\,(k)$ with k a field of characteristic prime to the order of G and that Y is smooth and projective over $\mathrm{Spec}\,(k)$. Assume that Y contains a k-rational point.

The following construction motivates our terminology: Take $A = \mathrm{Pic}^0(Y)$ (the Picard abelian variety of Y) and suppose we have a group scheme immersion $\phi : G^D \to A$. The k-rational point on Y provides us with a morphism $Y \to \mathrm{Alb}(Y)$ to the Albanese abelian variety of Y. Set $B = A/G^D$ for the quotient abelian variety and consider

$$0 \to G \to B^{\mathrm{dual}} \to A^{\mathrm{dual}} \to 0$$

given by the isogeny dual to $A \to B$. The canonical duality $A^{\mathrm{dual}} \simeq \mathrm{Alb}(Y)$ between the Albanese and Picard varieties of Y allows us to view this exact sequence as a G-torsor over $\mathrm{Alb}(Y)$. We can restrict this along $Y \to \mathrm{Alb}(Y)$ to obtain a G-torsor $X \to Y$. Such torsors are called of Albanese type by Lang [La]. One can now see (using for example [Mu] §15) that $X \to Y$ is also of Albanese type according to our definition above. The required extension

$$1 \to \mathbf{G}_{mY} \to \mathcal{E} \to A_Y \to 1 \tag{11.7}$$

is given as the pull-back along $Y \times_S A \to \mathrm{Alb}(Y) \times_S A \simeq A^{\mathrm{dual}} \times_S A$ of the extension over $A_{A^{\mathrm{dual}}} = A^{\mathrm{dual}} \times_S A$ given by the Poincare invertible sheaf with its biextension structure.

Theorem 11.4. *Suppose $S = \mathrm{Spec}\,(k)$ with k a field of characteristic prime to the order of G and that Y is smooth and projective over $\mathrm{Spec}\,(k)$. Assume that Y contains a k-rational point and let $X \to Y$ be a G-torsor such that X is geometrically connected. Then $X \to Y$ is of Albanese type if and only if all the torsion invertible sheaves $\mathcal{O}_{X,\chi}$, with χ running over all characters of G (see §2.d), correspond to divisors on $Y \times_k k(\chi)$ which are algebraically trivial, or equivalently if and only if it is obtained by pulling back a G-isogeny of the Albanese abelian variety $\mathrm{Alb}(Y)$ along $Y \to \mathrm{Alb}(Y)$.*

Proof. This follows from the construction and properties of the Picard and Albanese abelian varieties of Y as in Remark 11.3 (c) above. □

Remark 11.5. Assume that $X \to Y$ is an abelian G-torsor over the ring of integers $\mathcal{O}_K$ of the number field K such that the generic fiber $X_K \to Y_K$ is of Albanese type. Assume that Y_K is smooth and that $Y \to \mathrm{Spec}\,(\mathcal{O}_K)$ has a section. Let $\mathcal{A}^0$ be the connected component of the Neron model $\mathcal{A}$ of $\mathrm{Pic}^0(Y_K)$. It would be interesting to find conditions under which $X \to Y$ is of Albanese type over $\mathrm{Spec}\,(\mathcal{O}_K)$ with $A = \mathcal{A}^0$; this is always the case when Y_K is a curve of genus ≥ 2 and Y is regular by [Ra] §8.

Let $\pi : X \to Y$ be an (abelian) G-torsor of Albanese type over $S = \mathrm{Spec}\,(R)$. Suppose now that the residue fields of all the generic points of S are perfect. Denote by $h_A : Y \times_S A \to A$ the base change of $h : Y \to S$ and let $\mathcal{M}_A = \det(\mathbf{R}h_{A*}(\mathcal{P}))$, $\mathcal{M} = \det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))$ (invertible sheaves on A and G_S^D respectively). Since $\pi_*(\mathcal{O}_X) \simeq (\mathrm{id}_Y \times_S \phi)^*(\mathcal{P})$ we then have $\mathcal{M} \simeq \phi^*(\mathcal{M}_A)$. By [Br] Proposition 2.4 and the discussion before it (see also [SGA7I] VIII), the invertible sheaf $\mathcal{L}_A$ over A supports a canonical cubic structure (as in Definition 3.1 with $n = 3$). This statement is of course an extension to this situation of the classical theorem of the cube for line bundles over abelian varieties. (Notice that Breen uses a slightly different definition of cubic structure; see Remark 3.2 (a) or [Br] 2.8. However, it is not hard to see that this does not affect the truth of our statement.) Using the functoriality of cubic structures, we can conclude that $\mathcal{M} \simeq \phi^*(\mathcal{M}_A)$ also supports a cubic structure.

11.e. We can now complete the proof of our main results (Theorems 1.1, 1.2 and 1.3).

As in these statements we assume that G is a finite group and $\pi : X \to Y$ is a G-torsor with $h : Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d. We set $f = h \cdot \pi$ and $S = \mathrm{Spec}\,(\mathbf{Z})$.

A standard argument using Noetherian induction shows:

Lemma 11.6. *The Grothendieck group* $\mathrm{G}_0(Y)$ *is generated by the classes* $[i_*\mathcal{O}_Z]$ *with* $i : Z \hookrightarrow Y$ *an integral subscheme of* Y. *There are two possibilities for such a* Z*: Either the morphism* $Z \to \mathrm{Spec}\,(\mathbf{Z})$ *is flat of relative dimension* $d' \leq d$*, or it factors through* $\mathrm{Spec}\,(\mathbf{F}_p) \to \mathrm{Spec}\,(\mathbf{Z})$ *for some prime* p. □

Recall the descent isomorphism $\pi^* : G_0(Y) \xrightarrow{\sim} G_0(G, X)$. Let $i : Z \hookrightarrow Y$ be as in Lemma 11.6 and consider the G-torsor $\pi_Z : X \times_Y Z \to Z$ obtained by pulling back π along the closed immersion i. Denote by $f' : X \times_Y Z \to \mathrm{Spec}\,(\mathbf{Z})$ the structure morphism. Then it follows from the construction of the projective Euler characteristic that

$$\chi_f^P(\pi^*(i_*\mathcal{O}_Z)) = \chi_{f'}^P(\mathcal{O}_{X\times_Y Z}). \tag{11.8}$$

If $Z \to \mathrm{Spec}\,(\mathbf{Z})$ factors through $\mathrm{Spec}\,(\mathbf{F}_p) \to \mathrm{Spec}\,(\mathbf{Z})$ then it follows from the main theorem of [Na] that $\bar{\chi}_{f'}^P(\mathcal{O}_{X\times_Y Z}) = 0$ (see also [P] 4.b Remark 3). On the other hand, we notice that if $d' \leq d$ we have $M_{d'+1}(G)|M_{d+1}(G)$, $M'_{d'+1}(G)|M'_{d+1}(G)$ and also $C_{d'+1}(G)|C_{d+1}(G)$. Using Lemma 11.6, the additivity of the Euler characteristic $\bar{\chi}_f^P$ (Theorem 11.1) and (11.8), we can now see that the proofs of Theorems 1.1, 1.2 are reduced to the case that $\mathcal{F}$ is the structure sheaf $\mathcal{O}_X = \pi^*\mathcal{O}_Y$ and Y is integral. A similar argument using $(d'+1)!!|(d+1)!!$ for $d' \leq d$ together with Remark 11.3 (b) shows that the proof of Theorem 1.3 is also reduced to the case that $\mathcal{F}$ is the structure sheaf of X and Y is integral.

Let us first discuss the completion of the proofs of Theorems 1.1 and 1.2. This borrows heavily from the arguments in [P]: Noetherian induction and an argument as in the proof of [P] Proposition 4.4 (a) shows that $(\#G)^{d+1} \cdot \bar{\chi}^P(\mathcal{O}_X) = 0$. Suppose first that G is abelian. In this case, by Theorem 9.8, the invertible sheaf $\det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ over G_S^D supports a $d+2$-cubic structure. Hence, it follows from 11.4 and Theorem 7.10 that $\kappa \cdot \bar{\chi}^P(\mathcal{O}_X)$ is annihilated by $M_{d+1}(G)$. Since $(\#G)^{d+1} \cdot \bar{\chi}^P(\mathcal{O}_X) = 0$ this gives Theorem 1.1 (b) for

$\mathcal{F} = \mathcal{O}_X$ when G is abelian. In fact, we can see that when G is abelian and $\mathcal{F} = \mathcal{O}_X$, the conclusion of Theorem 1.1 (b) with $\epsilon(G)$ replaced by $\epsilon(G, Y)$ holds true.

The fact that $(\#G)^{d+1} \cdot \bar{\chi}^P(\mathcal{O}_X) = 0$ together with the "localization" argument in the proof of [P] Proposition 4.5 shows that the proofs of Theorems 1.1 and 1.2 in general reduce to the case that G is an l-group, l prime.

Theorem 1.1 (b) now follows from the abelian case just explained above. To show Theorem 1.1 (a) observe that the argument in [P] p. 215-216 allows us to reduce the case of an l-group to that of the case of a "basic" l-group with l odd, i.e to the case of a cyclic group of odd prime order l. Then part (a) follows once again by the abelian case. This completes the proof of Theorem 1.1.

The same argument from [P] also shows that the proof of Theorem 1.2 can be reduced to the case of a "basic" l-group with l odd, i.e to the case of a cyclic group of odd prime order l. Then Theorem 1.2 follows from Theorem 9.8 and Theorem 8.4. □

Let us now discuss the proof of Theorem 1.3. Recall that it is enough to deal with the case that $\mathcal{F} = \mathcal{O}_X$ and Y is integral. It is also enough to assume that $d \geq 1$. Let us first discuss part (a): Since $\pi : X \to Y$ is of Albanese type, by §11.d, the invertible sheaf $\mathcal{M} := \det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))$ supports a 3-cubic structure. Hence, by Corollary 7.11, $\mathcal{M}$ is trivial. It follows from (11.4) that $\bar{\chi}^P(\mathcal{O}_X) = 0$ in $\mathrm{Cl}(\mathbf{Z}[G])$. This completes the proof of part (a).

It remains to prove Theorem 1.3 (b):

For simplicity, we set $T = X_{\mathbf{Q}}$, $U = Y_{\mathbf{Q}}$. We are assuming that $T \to U$ is of Albanese type and so there is a commutative group scheme A and an extension $\mathcal{E}$ as in Definition 11.2. We denote by $\mathcal{P}$ the invertible sheaf over $A_U = U \times_{\mathbf{Q}} A$ given by $\mathcal{E}$. By Theorem 9.8, the invertible sheaf $\mathcal{M}^{\otimes 2} = \det \mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))^{\otimes 2}$ over G^D_S supports a $d{+}2$-cubic structure ξ. We can apply the same argument to the invertible sheaf $\mathcal{M}_A = \det(\mathbf{R}h_{A*}(\mathcal{P}))$ over A: Here we start from the extension

$$1 \to \mathbf{G}_{mU} \to \mathcal{E} \to A_U \to 1 \tag{11.9}$$

and the corresponding additive functor $A \to \mathcal{PIC}(U)$; in this case, we have to work using the fpqc topology. We obtain that $\mathcal{M}_A^{\otimes 2}$ has a canonical $d+2$-cubic structure ξ_A over A. Recall that the extension $\mathcal{E}$ pulls back to the extension

$$1 \to \mathbf{G}_{mU} \to E \to G^D_U \to 1 \tag{11.10}$$

using $\phi : G^D_{\mathbf{Q}} = G^D_{\mathrm{Spec}\,(\mathbf{Q})} \to A$. This implies that the $d+2$-cubic structure $\xi_{\mathbf{Q}}$ on the generic fiber $\mathcal{M}_{\mathbf{Q}}^{\otimes 2}$ (an invertible sheaf over $G^D_{\mathbf{Q}} = \mathrm{Spec}\,(\mathbf{Q}[G])$) is obtained by pulling back ξ_A along ϕ; so there is an isomorphism of $d+2$-cubic structures $\xi_{\mathbf{Q}} \simeq \phi^*(\xi_A)$. However, as a corollary of the theorem of the cube on A (see the argument at the end of the previous paragraph), $\mathcal{M}_A$ and hence also $\mathcal{M}_A^{\otimes 2}$ has a canonical 3-cubic structure. This induces a $d+2$-cubic structure ξ'_A on $\mathcal{M}_A^{\otimes 2}$ using the construction of Lemma 5.1. We claim that this agrees with the $d+2$-cubic structure ξ_A: To see this observe that the composition $\xi_A^{-1} \cdot \xi'_A$ is given by an invertible regular function c on A^{d+2} which gives a $d+2$-cubic structure on

the trivial invertible sheaf. By §3.b $(c0')$ we have $c(a_1,\dots,a_{d+2})=1$ if one of the a_i is zero. By a classical lemma of Rosenlicht ([SGA7] VIII 4.1) this implies that c is equal to 1. Hence $\xi'_A=\xi_A$. Since $\xi_{\mathbf{Q}}\simeq\phi^*(\xi_A)$ and $\xi'_A=\xi_A$ comes from a 3-cubic structure (using Lemma 5.1) we conclude that the same is true for $\xi_{\mathbf{Q}}$. Now we will consider the Taylor expansion of Corollary 5.6 for $(\mathcal{M}^{\otimes 2},\xi)$ and $(\mathcal{M}_{\mathbf{Q}}^{\otimes 2},\xi_{\mathbf{Q}})$ (we take $n=d+1$). For simplicity, set $\mathcal{L}=\mathcal{M}^{\otimes 2}$, $\mathcal{L}_{\mathbf{Q}}=\mathcal{M}_{\mathbf{Q}}^{\otimes 2}$. By repeated application of Lemma 5.2 and Proposition 5.4 we see that since $(\mathcal{L}_{\mathbf{Q}},\xi_{\mathbf{Q}})$ is a $d+2$-cubic structure which comes from a 3-cubic structure the $(d+1-i)$-extensions $E(\mathcal{L}_{\mathbf{Q}}^{(i)},\xi_{\mathbf{Q}}^{(i)})$ of $G_{\mathbf{Q}}^D$ by $\mathbf{G}_m$ are trivial when $d+1-i\geq 3$. Since the construction of $(\mathcal{L}^{(i)},\xi^{(i)})$ commutes with base change from $\mathbf{Z}$ to $\mathbf{Q}$, this now implies that the $(d+1-i)$-extensions $E(\mathcal{L}^{(i)},\xi^{(i)})$ of G^D by $\mathbf{G}_m$ (over $S=\mathrm{Spec}\,(\mathbf{Z})$) become trivial after base change to the generic fiber $\mathrm{Spec}\,(\mathbf{Q})$ when $d+1-i\geq 3$. We claim that this implies that all these multiextensions are trivial. To see this let us consider the commutative diagram

$$\begin{array}{ccccc} n\text{-}\mathrm{Ext}^1(G^D,\mathbf{G}_m) & \xrightarrow{\sim} & (n-1)\text{-}\mathrm{Ext}^1(G^D,G) & \xrightarrow{t} & \mathrm{H}^1((G^D)^{n-1},G) \\ \downarrow & & \downarrow & & \downarrow \\ n\text{-}\mathrm{Ext}^1(G^D_{\mathbf{Q}},\mathbf{G}_m) & \xrightarrow{\sim} & (n-1)\text{-}\mathrm{Ext}^1(G^D_{\mathbf{Q}},G) & \xrightarrow{t_{\mathbf{Q}}} & \mathrm{H}^1((G^D_{\mathbf{Q}})^{n-1},G). \end{array} \tag{11.11}$$

Here the isomorphisms on the left side are given by (6.12). The homomorphism t is the forgetful map; the bottom row is obtained by the constructions that give the first row but performed over $\mathrm{Spec}\,(\mathbf{Q})$. The vertical arrows are the base change homomorphisms. By Lemma 7.12 t is injective (the argument immediately extends to the case that G is not cyclic). The right vertical arrow is also injective. We conclude that the left vertical arrow is injective; this implies the desired result: the $(d+1-i)$-extensions $E(\mathcal{L}^{(i)},\xi^{(i)})$ of G^D by $\mathbf{G}_m$ (over $S=\mathrm{Spec}\,(\mathbf{Z})$) are trivial when $d+1-i\geq 3$. In addition, by Remark 7.9 (a) the $(d+1-i)$-extensions $E(\mathcal{L}^{(i)},\xi^{(i)})$ are trivial when $d+1-i<3$. This, together with $\mathrm{Pic}(S)=(0)$, implies that all the terms in the Taylor expansion of $\mathcal{L}^{\otimes(d+1)!!}$ are trivial. Hence, by (11.4), we have $2((d+1)!!)\cdot\bar{\chi}^P(\mathcal{O}_X)=0$ in $\mathrm{Cl}(\mathbf{Z}[G])$. This concludes the proof of Theorem 1.3. ◻

Remark 11.7. Suppose that Y is normal of dimension ≥ 2 and denote by

$$Y\xrightarrow{h'}S'=\mathrm{Spec}\,(\mathcal{O}_K)\xrightarrow{\phi}S=\mathrm{Spec}\,(\mathbf{Z}) \tag{11.12}$$

the "Stein factorization" of h where $\mathcal{O}_K$ is the ring of integers of the number field K. Assume that the abelian G-torsor $X\to Y$ is of Albanese type *as a torsor over* S'. Then the proof of Theorem 1.3 (a) above can be extended to show that $\bar{\chi}^P(\mathcal{F})=0$ in $\mathrm{Cl}(\mathbf{Z}[G])$. Similarly, if $X_K\to Y_K$ is of Albanese type over $\mathrm{Spec}\,(K)$ we can obtain that the conclusion of Theorem 1.3 (b) holds i.e that $2((d+1)!!)\cdot\bar{\chi}^P(\mathcal{F})=0$ for all G-equivariant $\mathcal{F}$ on X. To see this it is enough to combine the arguments for $h':Y\to S'$ above with the following observations:

i) There is a canonical isomorphism

$$\det\mathbf{R}h_{G^D*}(\pi_*(\mathcal{O}_X))\xrightarrow{\sim}\det(\phi_*(\det\mathbf{R}h'_{G^D*}(\pi_*(\mathcal{O}_X)))).$$

ii) For any invertible sheaf $\mathcal{M}'$ on $G^D_{S'}$ and $n \geq 2$ the additivity of the Norm (2.3 (b)) gives a canonical isomorphism

$$\mathfrak{N} : \mathrm{Norm}_{S'/S}(\Theta_n(\mathcal{M}')) \xrightarrow{\sim} \Theta_n(\det(\phi_*(\mathcal{M}'))).$$

iii) If $(\mathcal{M}', \xi')$ is an invertible sheaf with an n-cubic structure over $G^D_{S'}$ then the isomorphism $\xi := \mathfrak{N} \cdot \mathrm{Norm}_{S'/S}(\xi')$ defines an n-cubic structure on $\mathcal{M} := \det(\phi_*(\mathcal{M}'))$ over G^D_S.

We will leave the details to the reader.

Let us finish by explaining how we can deduce the other results stated in the introduction. Corollary 1.4 follows directly from Theorem 1.1 (b), Theorem 1.3 (a) and the definition of the projective Euler characteristic (Theorem 11.1). Notice that the improvement ($\epsilon(G, Y)$ in place of $\epsilon(G)$) in Theorem 1.1 (b) and Corollary 1.4 in the case that $\mathcal{F} = \mathcal{O}_X$ which was stated in the introduction follows now directly from the argument in the proof of Theorem 1.1 (b) above. Corollary 1.5 follows from Theorem 1.1 (b) and Theorem 1.3 (a) in exactly the same way as explained in the proof of [P] Cor. 5.3. Finally, if $G = \mathbf{Z}/p\mathbf{Z}$ with p odd and $p > d+1$ then the equality

$$\bar{\chi}^P(\mathcal{O}_X) = \sum_{i=1}^{d+1} R^{(i)}(t_i(X/Y))$$

of the introduction follows from (11.4) and (8.11) after setting $\mathcal{L} = \det \mathbf{R}h_{G^D *}(\pi_*(\mathcal{O}_X))^{\otimes\kappa}$ and $t_i(X/Y) = \kappa^{-1} t_i(\mathcal{L}, \xi) \in \mathrm{Hom}((C(p)/p)^{(1-i)}, \mathbf{Z}/p)$. This combined with Remark 10.4 (a) gives

$$t_{d+1}(X/Y) = \frac{1}{\kappa \cdot (d+1)!}[T(X/Y)] \tag{11.13}$$

where $[T(X/Y)]$ is the element that corresponds to the unramified $\mathbf{Z}/p$-extension of $\mathbf{Q}(\zeta_p)$ given in Proposition 10.3. $\square$

Remark 11.8. It follows from the proof of Theorem 1.3 and the construction of the elements $t_i(X/Y) = \kappa^{-1} t_i(\mathcal{L}, \xi)$ that these are trivial for $i \geq 3$ when Y is integral and $X_{\mathbf{Q}} \to Y_{\mathbf{Q}}$ is of Albanese type.

APPENDIX

In this appendix, we show how a well-known argument due to Godeaux and Serre ([Se] §20) combined with an "arithmetic" version of Bertini's theorem (based on the theorem of Rumely on the existence of integral points [Ru], [MB2]) allows us to construct "geometric" G-torsors $\pi : X \to Y$ with Y regular and $Y \to \mathrm{Spec}\,(\mathbf{Z})$ projective and flat of relative dimension d for any finite group G and any integer $d \geq 1$. In fact, for the G-torsors that we construct $Y \to \mathrm{Spec}\,(\mathbf{Z})$ factors through a smooth morphism $Y \to \mathrm{Spec}\,(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the ring of integers of a number field K.

To explain this set $L = \mathbf{Z}[G]$ and for an integer $r \geq 1$ we denote by $S(r) = \oplus_{m\geq 0} S(r)_m = \mathrm{Sym}_{\mathbf{Z}}(L^{\oplus r})$ the corresponding (graded) symmetric algebra with G-action. We set $X(r) = \mathbf{Proj}(S(r))$; this is then a projective space of (relative) dimension $s = r\cdot(\#G) - 1$ over $\mathrm{Spec}\,(\mathbf{Z})$ that supports a linear action of G. The quotient $Y(r) = X(r)/G$ is also a projective scheme: We can see that, for sufficiently large integers k,

$$Y(r) \simeq \mathbf{Proj}\Big(\bigoplus_{m\geq 0}(S(r)_{mk})^G\Big),$$

and the graded algebra $\bigoplus_{m\geq 0}(S(r)_{mk})^G$ is generated by the free $\mathbf{Z}$-module $M := S(r)_k^G$. Set $\mathbf{P}(M) = \mathbf{Proj}(\mathrm{Sym}(M))$; then $Y(r)$ is a closed subscheme of $\mathbf{P}(M)$. (The reader can consult [Se] §20 for the details of the argument in the corresponding situation over an algebraically closed field; the same argument readily applies to our case.) Denote by $\pi(r) : X(r) \to Y(r)$ the quotient morphism. Let $B(r)$ be the closed subscheme of $X(r)$ consisting of points with non-trivial inertia subgroups and set $b(r)$ for the (reduced) image $\pi(r)(B(r))$. The group G acts freely on the open subscheme $U(r) := X(r) - B(r)$, the morphism $\pi(r) : U(r) \to V(r) := Y(r) - b(r)$ is a G-torsor and $V(r) \to \mathrm{Spec}\,(\mathbf{Z})$ is smooth of relative dimension s. One can now observe ([Se]) that for all sufficiently large r, each fiber of $b(r) \to \mathrm{Spec}\,(\mathbf{Z})$ has codimension $> d$ in the corresponding fiber of $Y(r) \to \mathrm{Spec}\,(\mathbf{Z})$.

Now let us consider the dual projective space $\mathbf{P}(M^\vee)$ parametrizing hyperplane sections of $\mathbf{P}(M)$. Denote by $\mathbf{H} \subset \mathbf{P}(M) \times \mathbf{P}(M^\vee)$ the universal hyperplane section. Let us set $Q = (\mathbf{P}(M^\vee))^{s-d}$. For $\phi : T \to Q$, $i = 1, \ldots, s-d$, let $\mathbf{H}^i_\phi$ be the hyperplane in $\mathbf{P}(M) \times T$ that corresponds to $\mathrm{pr}_i \cdot \phi : T \to \mathbf{P}(M^\vee)$ (this is the Cartesian product

$$\begin{array}{ccc}
\mathbf{H}^i_\phi & \longrightarrow & \mathbf{H} \\
\big\downarrow & & \big\downarrow \\
\mathbf{P}(M) \times T & \xrightarrow{\mathrm{id}\times \mathrm{pr}_i\cdot\phi} & \mathbf{P}(M) \times \mathbf{P}(M^\vee).)
\end{array}$$

Set $Y(r)_{\phi:T\to Q}$ for the scheme theoretic intersection

$$(Y(r) \times T) \cap (\mathbf{H}^1_\phi \cap \cdots \cap \mathbf{H}^{s-d}_\phi)$$

in $\mathbf{P}(M) \times T$; this is a scheme over T. Let V_1 be the subset of $x \in Q$ for which

$$Y(r)_{\mathrm{Spec}\,(k(x))\to Q} \subset Y(r) \times \mathrm{Spec}\,(k(x))$$

does not intersects $b(r)\times\mathrm{Spec}\,(k(x))$. Let V_2 be the subset of $x\in Q$ for which the projection $Y(r)_{\mathrm{id}:Q\to Q}\to Q$ is flat at all points that lie over x. Finally, let V_3 be the subset of $x\in Q$ for which $Y(r)_{\mathrm{Spec}\,(k(x))\to Q}$ is smooth over $\mathrm{Spec}\,(k(x))$ of dimension d. Set $V=V_1\cup V_2\cup V_3$; this is a constructible subset of Q. The proof of the usual Bertini theorem (over fields) applies to show that V contains the generic point of each fiber $Q\to\mathrm{Spec}\,(\mathbf{Z})$. Therefore, the complement $Q-V$ is contained in a closed subscheme Z which is such that $Q-Z\to\mathrm{Spec}\,(\mathbf{Z})$ is surjective. By [Ru] or [MB2] there is a number field K with integer ring $\mathcal{O}_K$ and an integral point $\phi:\mathrm{Spec}\,(\mathcal{O}_K)\to Q-Z\subset Q$. Since $Q-Z\subset V$, the pull-back of $X(r)\to Y(r)$ via $Y(r)_\phi\to Y(r)\times\mathrm{Spec}\,(\mathcal{O}_K)$ now gives a G-torsor $X\to Y:=Y(r)_\phi$ with $Y\to\mathrm{Spec}\,(\mathcal{O}_K)$ projective and smooth of relative dimension d. The argument in [Se] now shows that the generic fiber X_K is geometrically connected.

References

[AHS] M. Ando, M. J. Hopkins, N. P. Strickland: Elliptic spectra, the Witten genus and the theorem of the cube. Invent. Math. **146** (2001), no. 3, 595–687.

[BM] H. Bass, M. P. Murthy: Grothendieck groups and Picard groups of abelian group rings. Annals of Math. **86** (1967), 16–73.

[Bo] A. Borel: Stable real cohomology of arithmetic groups. Ann. Sci. École Norm. Sup. (4) **7** (1974), 235–272.

[Br] L. Breen: *Fonctions thêta et théorème du cube.* Lecture Notes in Mathematics, Vol. 980. Springer-Verlag, Berlin-New York, 1983.

[BCEM] J. Buhler, R. Crandall, R. Ernvall and T. Metsänkylä: Irregular primes and cyclotomic invariants to 12 million. Computational algebra and number theory (Milwaukee, WI, 1996). J. Symbolic Comput. 31 (2001), no. 1-2, 89–96.

[C] T. Chinburg: Galois structure of de Rham cohomology of tame covers of schemes, Annals of Math., **139** (1994), 443–490. Corrigendum, Annals of Math., **140** (1994), 251.

[CEPT] T. Chinburg, B. Erez, G. Pappas, M. J. Taylor: ε-constants and the Galois structure of de Rham cohomology, Annals of Math., **146** (1997), 411–473.

[CPT1] T. Chinburg, G. Pappas, M. J. Taylor: ε-constants and the Galois structure of de Rham cohomology II. J. Reine Angew. Math. **519** (2000), 201–230.

[CPT2] T. Chinburg, G. Pappas, M. J. Taylor: Cubic structures and a Riemann-Roch formula for equivariant Euler characteristics. Preprint.

[C-TS] J.-L. Colliot-Thélène, J.-J. Sansuc: On the Chow groups of certain rational surfaces: a sequel to a paper of S. Bloch. Duke Math. J. 48 (1981), no. 2, 421–447.

[DG] M. Demazure, P. Gabriel: *Groupes algébriques.* Masson et Cie, Paris; Amsterdam, North-Holland, 1970.

[De] P. Deligne: Le déterminant de la cohomologie, in *Currents Trends in Arithmetical Algebraic Geometry.* Contemporary Mathematics, Vol. **67**, A.M.S. (1987).

[DF] W. Dwyer, E. Friedlander: Algebraic and étale K-theory. Trans. Amer. Math. Soc. **292** (1985), no. 1, 247–280.

[Du] F. Ducrot: Cube structures and intersection bundles. Preprint 2002. (Available at http://math.univ-angers.fr/∼ducrot).

[Fa] G. Faltings: *Lectures on the arithmetic Riemann-Roch theorem.* Annals of Mathematics Studies, 127. Princeton University Press, Princeton, NJ, 1992.

[F1] A. Fröhlich: Stickelberger without Gauss sums, in "Algebraic Number Fields". Proceedings of the Durham Symposium 1975. Academic Press London 1977, 133–191.

[F2] A. Fröhlich: *Galois Module Structure of Algebraic Integers.* Ergebnisse der Mathematik und ihrer Grenzgebiete. (3) 1. Springer-Verlag, Berlin, 1983.

[Fu] W. Fulton: *Intersection theory.* 2nd edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 2. Springer-Verlag, Berlin, 1998.

[Gr] C. Greither: *Cyclic Galois extensions of commutative rings.* Lecture Notes in Mathematics, Vol. 1534. Springer-Verlag, Berlin, 1992. x+145 pp.

[KM] F. Knudsen, D. Mumford: The Projectivity of the Moduli space of Stable Curves (I): Preliminary on "det" and "Div". Math. Scand., **39** (1975), 19–55.

[KMi] I. Kersten, J. Michaliček: On Vandiver's conjecture and $\mathbf{Z}_p$-extensions of $\mathbf{Q}(\zeta_{p^n})$. J. Number Theory 32 (1989), no. 3, 371–386.

[Ku] M. Kurihara: Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$. Compositio Math. **81** (1992), no. 2, 223–236.

[La] S. Lang: Unramified class field theory over function fields in several variables. Ann. of Math. (2) 64 (1956), 285–325.

[L-MB] G. Laumon, L. Moret-Bailly: *Champs algébriques*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. 39. Springer-Verlag, Berlin, 2000.

[LS] R. Lee, R. H. Szczarba: On the torsion in $K_4(\mathbf{Z})$ and $K_5(\mathbf{Z})$. Duke Math. J. **45** (1978), no. 1, 101–129; with an addendum by C. Soulé. 131–132.

[M] B. Mazur: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. No. **47**, (1977), 33–186 (1978).

[MW] B. Mazur, A. Wiles: Class fields of abelian extensions of $\mathbf{Q}$. Invent. Math. **76** (1984), no. 2, 179–330.

[MB1] L. Moret-Bailly: *Pinceaux de variétés abéliennes*. Astérisque No. **129** (1985), 266 pp.

[MB2] L. Moret-Bailly: Groupes de Picard et problémes de Skolem. I, II. Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 2, 161–179, 181–194.

[Mu] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Oxford University Press, London 1970 viii+242 pp.

[Na] S. Nakajima: On Galois module structure of the cohomology groups of an algebraic variety. Invent. Math. **75** (1984), no. 1, 1–8.

[P] G. Pappas: Galois modules and the theorem of the cube. Invent. Math. **133** (1998), no. 1, 193–225.

[Ra] M. Raynaud: Spécialisation du foncteur de Picard. Inst. Hautes Études Sci. Publ. Math. No. 38, (1970), 27–76.

[Ri] D. S. Rim: Modules over finite groups. Annals of Math., **69** (1959), 700–712.

[Ro] J. Rognes: $K_4(\mathbf{Z})$ is the trivial group. Topology **39** (2000), no. 2, 267–281.

[Ru] R. Rumely: Arithmetic over the ring of all algebraic integers. J. Reine Angew. Math. **368** (1986), 127–133.

[Se] J.-P. Serre: Sur la topologie des variétés algébriques en caractéristique p. 1958 Symposium internacional de topologia algebraica (International symposium on algebraic topology) pp. 24–53. Universidad Nacional Autónoma de México and UNESCO, Mexico City. (Also in "J.-P. Serre, Collected Works", Springer-Verlag.)

[So] C. Soulé: Perfect forms and the Vandiver conjecture. J. Reine Angew. Math. **517** (1999), 209–221.

[Sw] R. G. Swan: Induced representations and projective modules. Annals of Math. **71** (1960), 552–578.

[SGA4] *Théorie des topos et cohomologie étale des schémas.* Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat. Lecture Notes in Mathematics, Vol. 269, 270, 305. Springer-Verlag, Berlin-New York, 1972-73.

[SGA6] *Théorie des intersections et théorème de Riemann-Roch*. Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre. Lecture Notes in Mathematics, Vol. 225. Springer-Verlag, Berlin-New York, 1971.

[SGA7I] *Groupes de monodromie en géométrie algébrique. I.* Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin-New York, 1972.

[Ta] M. J. Taylor: On Fröhlich's conjecture for rings of integers of tame extensions. Invent. Math. **63** (1981), no. 1, 41–79.

[W] L. Washington: *Introduction to cyclotomic fields*. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1982. xi+389 pp.

[Wa] W. Waterhouse: Principal homogeneous spaces and group scheme extensions. Trans. Amer. Math. Soc. **153** (1971), 181–189.

Dept. of Mathematics, Michigan State University, E. Lansing, MI 48824-1027, USA

E-mail address: `pappas@math.msu.edu`